Thecus

N8900 series/N12000 series/N16000 series
N5550/N6850/N8850/N10850
N7700PRO V2/N8800PRO V2
N4510U/N7510

User's Manual

Copyright and Trademark Notice
Thecus and other names of Thecus products are registered trademarks of Thecus Technology Corp. Microsoft, Windows, and the Windows logo are registered trademarks of Microsoft Corporation. Apple, iTunes and Apple OS X are registered trademarks of Apple Computers, Inc. All other trademarks and brand names are the property of their respective owners. Specifications are subject to change without notice.

Copyright © 2013 Thecus Technology Corporation. All rights reserved.

About This Manual

All information in this manual has been carefully verified to ensure its correctness. In case of an error, please provide us with your feedback. Thecus Technology Corporation reserves the right to modify the contents of this manual without notice.

Product name: Thecus N8900 / N12000 / N16000 series/N6850/N8850/N10850/N7700PRO V2/N8800PRO V2/N5550/N4510U/N7510
Manual Version: 5.3
Release Date: May 2013

Limited Warranty

Thecus Technology Corporation guarantees all components of Thecus NAS products are thoroughly tested before they leave the factory and should function normally under general usage. In case of any system malfunctions, Thecus Technology Corporation and its local representatives and dealers are responsible for repair without cost to the customer if the product fails within the warranty period and under normal usage. Thecus Technology Corporation is not responsible for any damage or loss of data deemed to be caused by its products. It is highly recommended that users conduct necessary back-up practices.

Check the functions that are available on your particular Thecus NAS model at:

http://www.Thecus.com

Safety Warnings

For your safety, please read and follow the following safety warnings:

- Read this manual thoroughly before attempting to set up your Thecus IP storage.
- Your Thecus IP storage is a complicated electronic device. DO NOT attempt to repair it under any circumstances. In the case of malfunction, turn off the power immediately and have it repaired at a qualified service center. Contact your vendor for details.
- DO NOT allow anything to rest on the power cord and DO NOT place the power cord in an area where it can be stepped on. Carefully place connecting cables to avoid stepping or tripping on them.
- Your Thecus IP storage can operate normally under temperatures between 5°C and 40°C, with relative humidity of 20% – 85%. Using Thecus IP storage under extreme environmental conditions could damage the unit.
- Ensure that the Thecus IP storage is provided with the correct supply voltage (AC 100V ~ 240V, 50/60 Hz, 3A). Plugging the Thecus IP storage to an incorrect power source could damage the unit.
- Do NOT expose Thecus IP storage to dampness, dust, or corrosive liquids.
- Do NOT place Thecus IP storage on any uneven surfaces.
- DO NOT place Thecus IP storage in direct sunlight or expose it to other heat sources.
- DO NOT use chemicals or aerosols to clean Thecus IP storage. Unplug the power cord and all connected cables before cleaning.
- DO NOT place any objects on the Thecus IP storage or obstruct its ventilation slots to avoid overheating the unit.
- Keep packaging out of the reach of children.
- If disposing of the device, please follow your local regulations for the safe disposal of electronic products to protect the environment.

Table of Contents

About This Manual **2**
Limited Warranty **2**
Safety Warnings **3**
Table of Contents **4**
Chapter 1: Introduction **7**
Overview **7**
Product Highlights **7**
Package Contents **9**
Front Panel **10**
Rear Panel **21**
Chapter 2: Hardware Installation **33**
Overview **33**
Before You Begin **33**
Cable Connections **33**
Chapter 3: First Time Setup **37**
Overview **37**
Thecus Setup Wizard **37**
LCD Operation (N7700PRO V2/N8800PRO V2/N5550/N4510U/N7510) **39**
OLED Operation(Does not apply to the N7700PRO V2/N8800PRO V2/N5550/N4510U/N7510) **41**
USB Copy **41**
Typical Setup Procedure **42**
Chapter 4: System Administration **44**
Overview **44**
Web Administration Interface **44**
My Favorite 45
Logout 47
Language Selection 47
System Information **48**
System Information 48
System/Service Status (Refer Chapter 7 for FW v2.03.01 and after) 48
Logs 49
On-line Register 50
Syslog Management 51
System Monitor 52
System Management **55**
Time: Setting system time 55
Notification configuration 55
Firmware Upgrade 56
Schedule Power On/Off 57
Administrator Password 58
Config Mgmt 58
Factory Default 59
Reboot & Shutdown 59
File System Check 59
Wake-Up On LAN (WOL) 61
SNMP Support 61
UI Login Function 62
System Network **63**

Networking 63
DHCP/RADVD 64
Linking Aggregation 65
Additional LAN 67
Storage Management 68
Disks Information (Refer Chapter 7 for FW v2.03.01 and after) 68
RAID Information 70
NAS Stacking 84
ISO Mount 90
Share Folder 93
Folder and sub-folders Access Control List (ACL) 96
iSCSI 98
iSCSI Thin-Provisioning 104
LUN ACL 105
Advance Option 106
High-Availability (N8900, N12000 series/N16000 series only) 108
User and Group Authentication 117
ADS/NT Support 117
Local User Configuration 119
Local Group Configuration 121
Batch Users and Groups Creation 123
User Quota 124
User and Group Backup 124
LDAP Support 125
Network Service 125
Samba / CIFS 125
AFP (Apple Network Setup) 128
NFS Setup 129
FTP 129
TFTP 130
WebService 131
UPnP 131
Bonjour Setting 132
SSH 132
DDNS 133
UPnP Port Management 134
Application Server 135
iTunes® Server 136
Module Installation 136
Auto Module Installation 137
Backup 138
Dual DOM (N12000 series/N16000 series/N8900 series only) 138
Rsync Target Server 139
Data Guard (Remote Backup) 140
ACL Backup and Restore 151
Data Burn 152
Thecus Backup Utility 155
Windows XP Data Backup 156
Apple OS X Backup Utilities 157
External Devices 157
Printers 157
Uninterrupted Power Source 162
Chapter 5: Tips and Tricks 162
USB and eSATA Storage Expansion 162
Remote Administration 163
Part I - Setup a DynDNS Account 164
Part II - Enable DDNS on the Router 164

Part III - Setting up Virtual Servers (HTTPS) 164
Firewall Software Configuration 164
Replacing Damaged Hard Drives 165
Hard Drive Damage 165
Replacing a Hard Drive 165
RAID Auto-Rebuild 165
Chapter 6: Troubleshooting 166
Forgot My Network IP Address 166
Can't Map a Network Drive in Windows XP 166
Restoring Factory Defaults 166
Problems with Time and Date Settings 167
Dual DOM Supports for Dual Protection (N12000 series/N16000 series/N8900 series only) 167
Chapter 7: Updates for FW v2.03.01 168
General 168
Status 168
Added Hardware Information 169
Disk Information 169
Data Guard (Local Backup) 172
Volume Expansion Management 188
Appendix A: Customer Support 189
Appendix B: RAID Basics 190
Overview 190
Benefits 190
Improved Performance 190
Data Security 190
RAID Levels 190
Appendix C: How to open the top cover 193
N8900 series: 193
N12000 series: 194
N16000 series: 194
Appendix D: Active Directory Basics 195
Overview 195
What is Active Directory? 195
ADS Benefits 195
Appendix E: Licensing Information 196
Overview 196
Source Code Availability 196
CGIC License Terms 197
GNU General Public License 197

Chapter 1: Introduction

Overview

Thank you for choosing the Thecus IP Storage Server. The Thecus IP storage is an easy-to-use storage server that allows a dedicated approach to storing and distributing data on a network. Data reliability is ensured with RAID features that provide data security and recovery—over multiple Terabyte of storage are available using RAID 5 and RAID 6. Gigabit Ethernet ports enhance network efficiency, allowing Thecus IP storage to take over file management functions, increase application and data sharing and provide faster data response. The Thecus IP storage offers data mobility with a disk roaming feature that lets you swap working hard drives for use in other Thecus IP storage, securing the continuity of data in the event of hardware failure. The Thecus IP storage allows data consolidation and sharing between Windows (SMB/CIFS), UNIX/Linux, and Apple OS X environments. The Thecus IP storage's user-friendly GUI supports multiple Languages.

Product Highlights

File Server

First and foremost, the Thecus IP storage allows you to store and share files over an IP network. With a Network Attached Storage (NAS) device, you can centralize your files and share them easily over your network. With the easy-to-use web-based interface, users on your network can access these files in a snap.

To learn about the Web User Interface, go to
Chapter 4: Using the Thecus IP Storage > Web Administration Interface

FTP Server

With the built-in FTP Server, friends, clients, and customers can upload and download files to your Thecus IP storage over the Internet with their favorite FTP programs. You can create user accounts so that only authorized users have access.

To set up the FTP Server, refer to
Chapter 4: Network Service> FTP .

iTunes Server

With the built-in iTunes server capability, the Thecus IP storage enables digital music to be shared and played anywhere on the network!

To set up the iTunes Server, refer to
Chapter 4: Application Server>iTunes Configuration.

Printer Server

With the Thecus IP storage's Printer Server, you can easily share an IPP printer with other PCs connected to your network.

To set up the Printer Server, refer to
Chapter 4: External Devices Server>Printer Information.

Multiple RAID

Thecus IP storage supports multiple RAID volumes on one system. So, you can create RAID 0 for your non-critical data, and create RAID 1,5,6,50 or 60 (depend on model) for mission-critical data. Create the RAID levels depending on your needs.

To configure RAID modes on the Thecus IP storage, refer to
Chapter 4: Storage Management >RAID Information.

iSCSI Capability

Thecus IP storage is not only a file server, but it also supports iSCSI initiators. Your server can access Thecus IP storage as a direct-attached-storage over the LAN or Internet. There is no easier way to expand the capacity of your current application servers. All the storage needs can be centrally managed and deployed. This brings ultimate flexibility to users.

To set up an iSCSI volume, refer to
Chapter 4: Storage Management > iSCSI

Superior Power Management

Thecus IP storage supports schedule power on/off. With this feature, administrator can set at what time to turn on or off the system. This feature is a big plus for people who want to conserve energy. Wake-On-LAN enables administrator to remotely turn on the system without even leaving their own seat.

To schedule system on and off, refer to
Chapter 4: System Management> Scheduled Power On/Off

Package Contents

N8900/N12000/N16000 Series/N8800PRO V2/N4510U-R

The Thecus IP storage should contain the following common items:

- System Unit x1
- QIG (Quick Installation Guide) x1
- CD-Title (Acronis backup CD & Universal CD & TwonkyMedia CD)
- Ethernet Cable x1
- Accessory bag x1
- HDD Compatibility list Card x1
- Multiple Languages Warranty Card x1
- Power cord x2

N6850/N8850/N10850/N7700PRO V2/N5550/N4510U-S/N7510

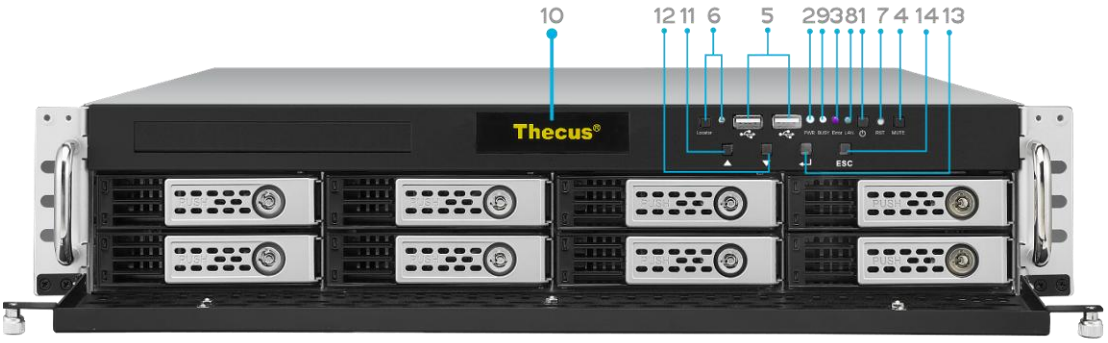
The Thecus IP storage should contain the following common items:

- System Unit x1
- QIG (Quick Installation Guide) x1
- CD-Title (Acronis backup CD & Universal CD & TwonkyMedia CD)
- Ethernet Cable x1
- Accessory bag x1
- HDD Compatibility list Card x1
- Multiple Languages Warranty Card x1
- Power cord x1

Please check to see if your package is complete. If you find that some items are missing, contact your dealer.

Front Panel

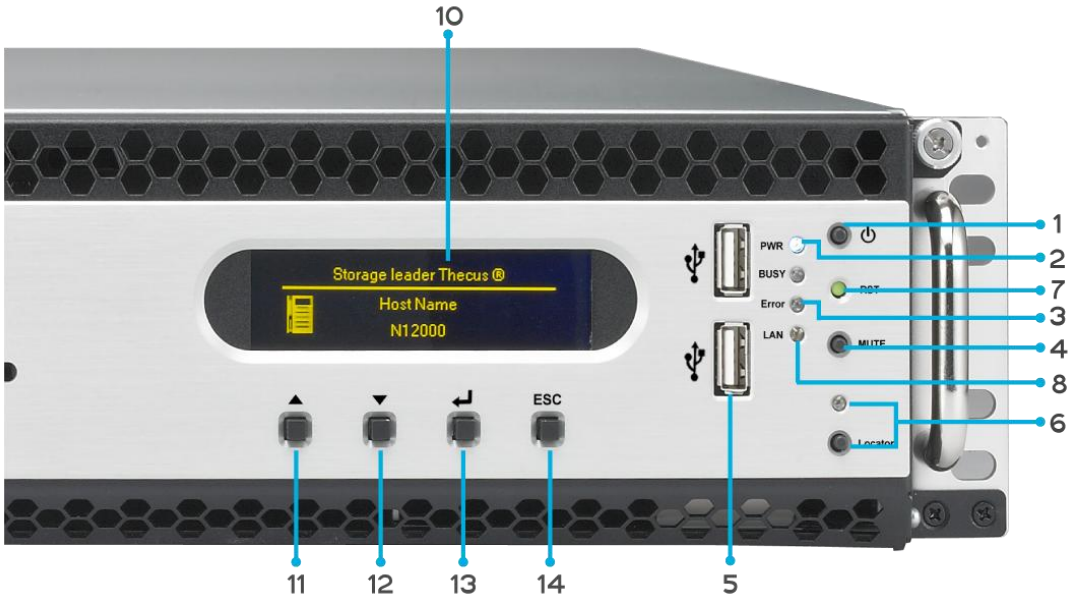
N8900 series:



Front Panel	
Item	**Description**
1.Power Button	• Power on/off N8900
2.Power LED	• **Solid green:** System is power on.
3.System error LED	• Solid RED: System error.
4.Mute button	• Mute the system fan alarm.
5.USB Port	• USB 2.0 port for compatible USB devices, such as USB disks and USB printers
6. Locator button / LED	• Press the button, the back led will light up to identify the system position of the rack
7. RST	• Reboot system.
8. LAN	• Blinking green: network activity • Solid green: network link
9. BUSY	• Blinking orange: system startup or system maintenance; data currently inaccessible
10.OLED	• Displays current system status and messages • OLED screen saver will be enabled after screen is idle for more than 3 minutes • OLED screen will be turn off after idle for more than 6 minutes
11.Up Button ▲	• Push to scroll up when using the OLED display
12.Down Button ▼	• Push to enter USB copy operation screen
13.Enter Button ↵	• Push to enter OLED operate password for basic system setting
14.Escape Button **ESC**	• Push to leave the current OLED menu

N12000 series:

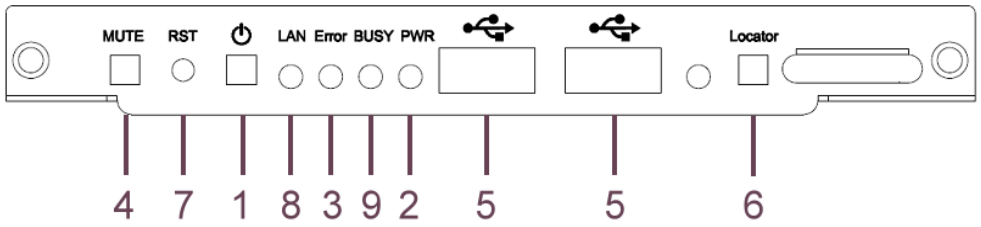
The Thecus N12000 series front panel has the device's controls, indicators, and hard disk trays:



Front Panel	
Item	**Description**
1.Power Button	• Power on/off N12000
2.Power LED	• **Solid green:** System is power on.
3.System error LED	• Solid RED: System error.
4.Mute button	• Mute the system fan alarm.
5.USB Port	• USB 2.0 port for compatible USB devices, such as USB disks and USB printers
6. Locator button / LED	• Press the button, the back led will light up to identify the system position of the rack
7. RST	• Reboot system.
8. LAN	• Blinking green: network activity • Solid green: network link
9. BUSY	• Blinking orange: system startup or system maintenance; data currently inaccessible
10.OLED	• Displays current system status and messages • OLED screen saver will be enabled after screen is idle for more than 3 minutes • OLED screen will be turn off after idle for more than 6 minutes
11.Up Button ▲	• Push to scroll up when using the OLED display
12.Down Button ▼	• Push to enter USB copy operation screen
13.Enter Button ↵	• Push to enter OLED operate password for basic system setting
14.Escape Button **ESC**	• Push to leave the current OLED menu

N16000 series:

The Thecus N16000 series front panel has the device's controls, indicators, and hard disk trays:



Front Panel	
Item	**Description**
1.Power Button	• Power on/off N16000
2.Power LED	• **Solid green:** System is power on.
3.System error LED	• Solid RED: System error.
4.Mute button	• Mute the system fan alarm.
5.USB Port	• USB 2.0 port for compatible USB devices, such as USB disks and USB printers
6. Locator button / LED	• Press the button, the back led will light up to identify the rack position of the system
7. RST	• Reboot system.
8. LAN	• Blinking green: network activity • Solid green: network link
9. BUSY	• Blinking orange: system startup or system maintenance; data currently inaccessible
10.OLED	• Displays current system status and messages • OLED screen saver will be enabled after screen is idle for more than 3 minutes • OLED screen will be turn off after idle for more than 6 minutes
11.Up Button ▲	• Push to scroll up when using the OLED display
12.Down Button ▼	• Push to enter USB copy operation screen
13.Enter Button ↵	• Push to enter OLED operate password for basic system setting
14.Escape Button **ESC**	• Push to leave the current OLED menu

N6850:

The Thecus N6850's front panel has the device's controls, indicators, and hard disk trays:

Front Panel	
Item	**Description**
1. Power Button	• Power on/off N6850
2. USB Port	• USB 2.0 port for compatible USB devices, such as digital cameras, USB disks, and USB printers.
3. USB Port	• USB 3.0 port for compatible USB devices, such as digital cameras, USB disks, and USB printers.
4. LAN2 LED	• **Solid white:** LAN2 Cable link • **Blinking :** Network activity
5. LAN1 LED	• **Solid white:** LAN1 Cable link • **Blinking :** Network activity
6. USB LED	• **Solid white:** USB busy • **Solid Red:** USB error
7. System LED	• **Solid white:** System is power on.
8. OLED	• Displays system status and information
9. System Error LED	• **Blinking RED:** System error.
10. Down Button	• Push to enter USB copy operation screen
11. Up Button	• Push to scroll up when using the OLED display
12. Enter Button	• Push to enter OLED operate password for basic system setting
13. Escape Button	• Push to leave the current OLED menu

N8850:

The Thecus N8850's front panel has the device's controls, indicators, and hard disk trays:

Front Panel	
Item	**Description**
1. Power Button	• Power on/off N8850
2. USB Port	• USB 2.0 port for compatible USB devices, such as digital cameras, USB disks, and USB printers.
3. USB Port	• USB 3.0 port for compatible USB devices, such as digital cameras, USB disks, and USB printers.
4. LAN2 LED	• **Solid white:** LAN2 Cable link • **Blinking :** Network activity
5. LAN1 LED	• **Solid white:** LAN1 Cable link • **Blinking :** Network activity
6. USB LED	• **Solid white:** USB busy • **Solid Red:** USB error
7. System LED	• **Solid white:** System is power on.
8. OLED	• Displays system status and information
9. System Error LED	• **Blinking RED:** System error.
10. Down Button	• Push to enter USB copy operation screen
11. Up Button	• Push to scroll up when using the OLED display
12. Enter Button	• Push to enter OLED operate password for basic system setting
13. Escape Button	• Push to leave the current OLED menu

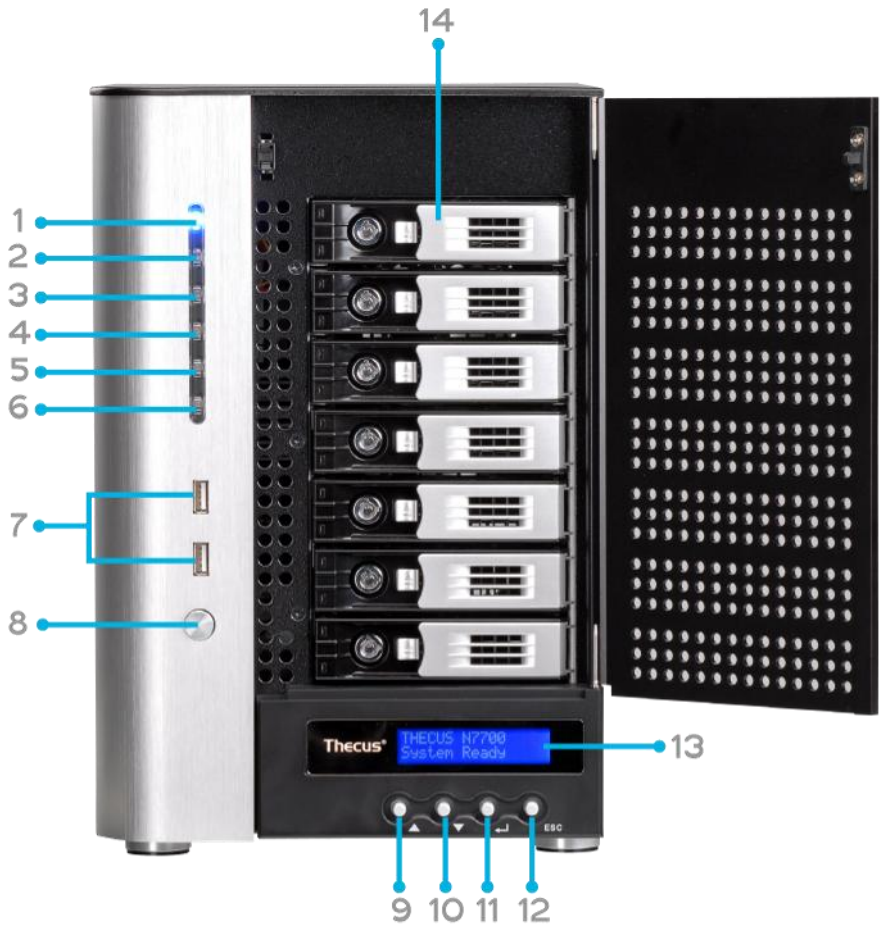
N10850:

The Thecus N10850's front panel has the device's controls, indicators, and hard disk trays:

Front Panel	
Item	**Description**
1. Power Button	• Power on/off N10850
2. USB Port	• USB 2.0 port for compatible USB devices, such as digital cameras, USB disks, and USB printers.
3. USB Port	• USB 3.0 port for compatible USB devices, such as digital cameras, USB disks, and USB printers.
4. LAN2 LED	• **Solid white:** LAN2 Cable link • **Blinking :** Network activity
5. LAN1 LED	• **Solid white:** LAN1 Cable link • **Blinking :** Network activity
6. USB LED	• **Solid white:** USB busy • **Solid Red:** USB error
7. System LED	• **Solid white:** System is power on.
8. OLED	• Displays system status and information
9. System Error LED	• **Blinking RED:** System error.
10. Down Button	• Push to enter USB copy operation screen
11. Up Button	• Push to scroll up when using the OLED display
12. Enter Button	• Push to enter OLED operate password for basic system setting
13. Escape Button	• Push to leave the current OLED menu

N7700PRO V2:

The Thecus N7700PRO V2 front panel has the device's controls, indicators, and hard disk trays:



Front Panel	
Item	**Description**
1.Power LED	• **Solid blue:** System is power on.
2.System LED	• **Solid orange:** system is being upgraded or system startup; data currently inaccessible
3.WAN/LAN1 LED	• **Solid green:** network link • **Blinking green:** network activity
4.LAN2 LED	• **Solid green:** network link • **Blinking green:** network activity
5.USB Copy LED	• **Solid blue:** files are being copied from a USB storage device
6.eSATA link LED	• **Solid blue:** external eSATA device has connected
7.USB Port	• USB 2.0 port for compatible USB devices, such as USB disks.
8.Power Button	• Power on/off N7700PRO V2
9.Up Button ▲	• Push to scroll up when using the LCD display
10.Down Button ▼	• Push to enter USB copy operation screen
11.Enter Button ↵	• Push to enter LCD operate password for basic system setting
12.Escape Button **ESC**	• Push to leave the current LCD menu
13.LCD Display	• Displays current system status and warning messages
14.HDD Trays	• Seven 3.5" SATA HDD trays • Locks are provided for added security

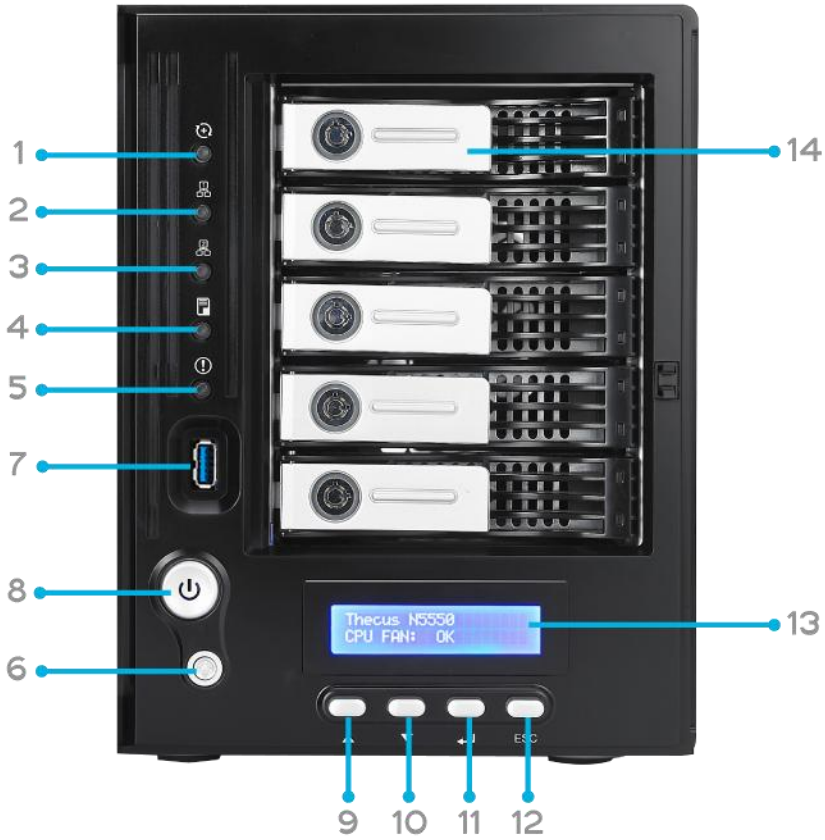
N8800PRO V2:

The Thecus N8800PRO V2 front panel has the device's controls, indicators, and hard disk trays:

Front Panel	
Item	**Description**
1.Power Button	• Power on/off N8800PRO V2
2.Power LED	• **Solid green:** System is power on.
3.Reboot Button	• Press to system reboot
4.System fan alarm LED	• **Solid red:** system fan failure notification
5. Mute button	• Mute the system fan alarm.
6.USB Port	USB 2.0 port for compatible USB devices, such as USB disks, USB printers
7.Up Button ▲	• Push to scroll up when using the LCD display
8.Down Button ▼	• Push to enter USB copy operation screen
9.Enter Button ↵	• Push to enter LCD operate password for basic system setting
10.Escape Button **ESC**	• Push to leave the current LCD menu

N5550:

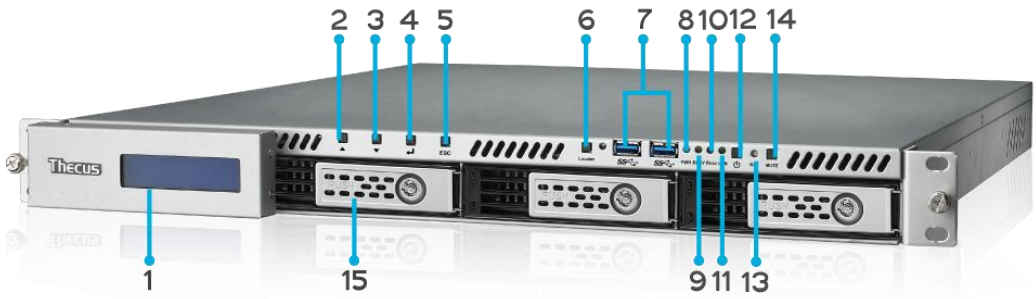
The Thecus N5550 front panel has the device's controls, indicators, and hard disk trays:



Front Panel	
Item	**Description**
1.System LED	• **Blinking orange:** System is being upgraded or ;is starting up; data currently inaccessible
2.WAN/LAN1 LED	• **Solid green:** Network link • **Blinking green:** Network activity
3.LAN2 LED	• **Solid green:** Network link • **Blinking green:** Network activity
4.USB Copy LED	• **Solid blue:** Files are being copied from a USB storage device
5.Syetem Warning LED	• **Solid RED:** System error
6.Reset Button	• Resets system configuration to default value.
7.USB Port	• USB 3.0 port for compatible USB devices, such as USB disks.
8.Power Button/ Power LED	• Power on/off N5550 and Power LED. • **Solid blue:** System is power on.
9.Up Button ▲	• Push to scroll up when using the LCD display.
10.Down Button ▼	• Push to enter the USB copy operation screen.
11.Enter Button ↵	• Push to enter LCD administrator password to access basic system setting.
12.Escape Button **ESC**	• Push to leave the current LCD menu.
13.LCD Display	• Displays current system status and warning messages.
14.HDD Trays	• Five 3.5" SATA HDD trays. • Locks are provided for added security.

N4510U:

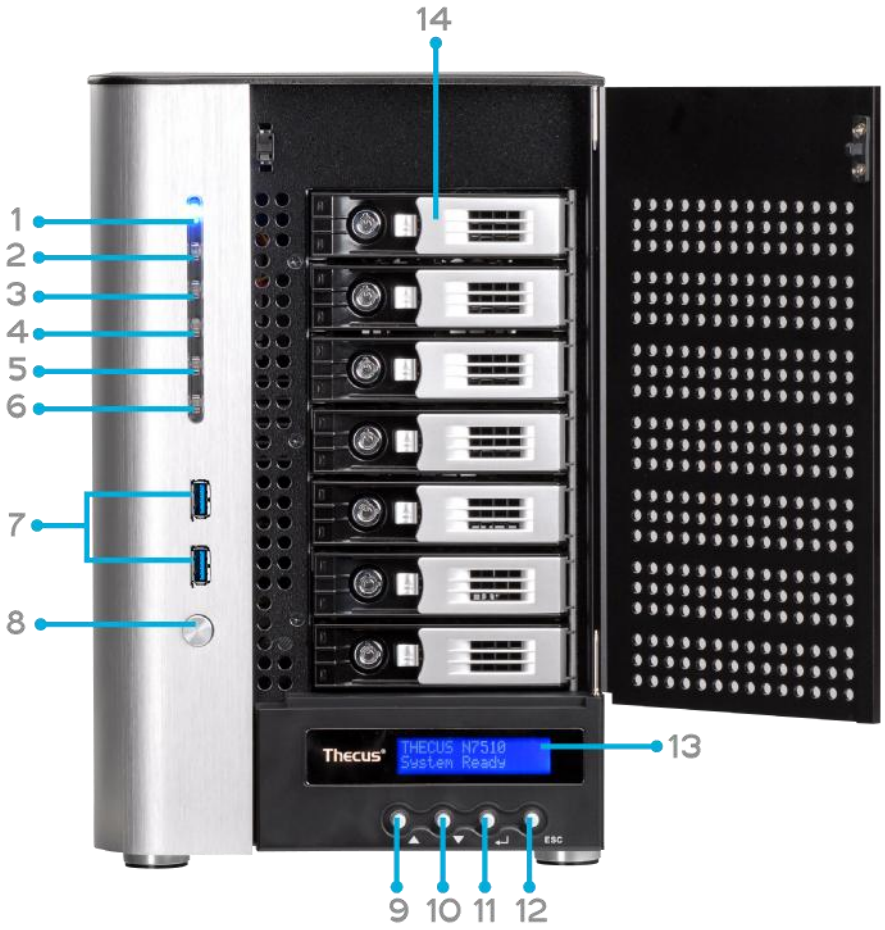
The Thecus N4510U front panel has the device's controls, indicators, and hard disk trays:



Front Panel	
Item	**Description**
1. LCD Display	• Displays the current system status and warning messages. • Displays hostname, WAN/LAN1/LAN2 IP addresses, RAID status, and current time.
2. Up Button ▲	• Push to scroll up when using the LCD display.
3. Down Button ▼	• Push to scroll down when using the LCD display.
4.Enter Button ↵	• Push to confirm information entered into the LCD display.
5. Escape Button **ESC**	• Push to leave the current LCD menu.
6. Locator Button	• Turns on the LED backlight.
7. USB Port	• USB 3.0 port for compatible USB devices, such as digital cameras, USB disks, and USB printers.
8. PWR LED	• **Solid Blue:** System is powered on.
9. Busy LED	• **Blinking orange:** system startup or system maintenance; data currently inaccessible
10. Error LED	**Solid Red:** System alert: Redundant power or system fan failure
11. LAN LED	• **Solid green:** network link • **Blinking green:** network activity
12. Power Button	• Power the N4510U on/off.
13. Reset Button	• Resets the N4510U.
14. Mute Button	• Mutes the system fan alarm (Can also be managed through the UI)
15. HDD Trays	• Four 3.5" SATA HDD trays. • Locks are provided for added security.

N7510:

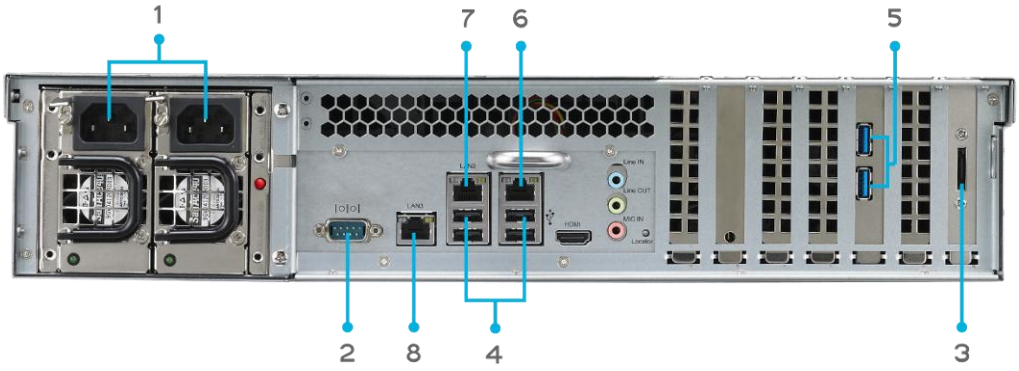
The Thecus N7510 front panel has the device's controls, indicators, and hard disk trays:



Front Panel	
Item	**Description**
1.Power LED	• **Solid blue:** System is power on.
2.System LED	• **Solid orange:** system is being upgraded or system startup; data currently inaccessible
3.WAN/LAN1 LED	• **Solid green:** network link • **Blinking green:** network activity
4.LAN2 LED	• **Solid green:** network link • **Blinking green:** network activity
5.USB Copy LED	• **Solid blue:** files are being copied from a USB storage device
6.eSATA link LED	• **Solid blue:** external eSATA device has connected
7.USB Port	• USB 3.0 port for compatible USB devices, such as USB disks.
8.Power Button	• Power on/off N7510
9.Up Button ▲	• Push to scroll up when using the LCD display
10.Down Button ▼	• Push to enter USB copy operation screen
11.Enter Button ↵	• Push to enter LCD operate password for basic system setting
12.Escape Button **ESC**	• Push to leave the current LCD menu
13.LCD Display	• Displays current system status and warning messages
14.HDD Trays	• Seven 3.5" SATA HDD trays • Locks are provided for added security

Rear Panel

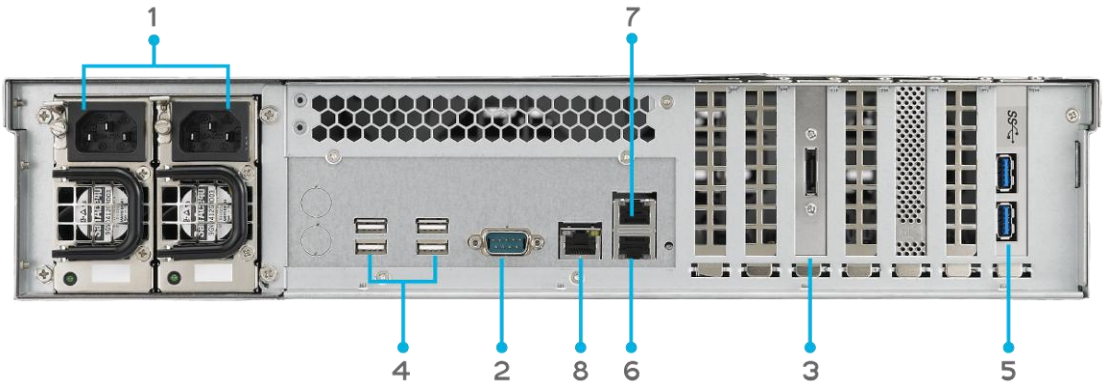
N8900



Back Panel	
Item	**Description**
1.Power Connector	• Connect the included power cords to these connectors
2.Serial Port	• This port is for external UPS device
3.eSATA Port	• eSATA port for high-speed storage expansion
4.USB Port	• USB 2.0 port for compatible USB devices, such as USB disks, and USB printers
5.USB Port	• USB 3.0 port for compatible USB devices.
6.WAN/LAN1 Port	• WAN/LAN1 port for connecting to an Ethernet network through a switch or router
7.LAN2 Port	• LAN2 port for connecting to an Ethernet network through a switch or router
8.LAN3 Port	• LAN3 port for connecting to an Ethernet network through a switch or router.

N12000:

The N12000 rear panel features ports and connectors.

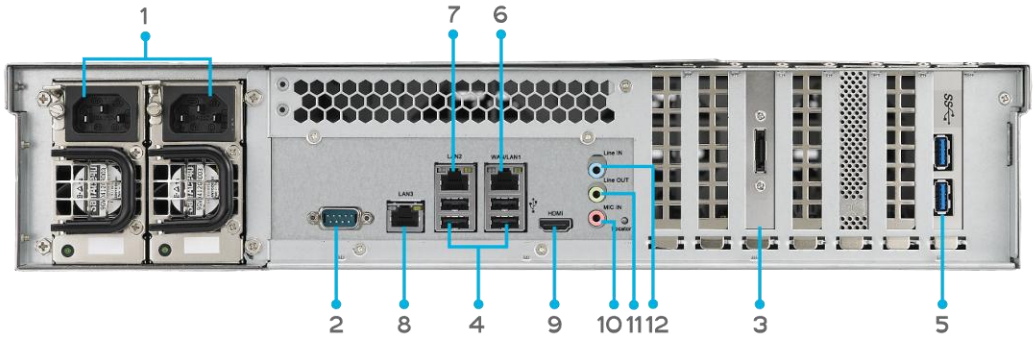


Back Panel	
Item	**Description**
1.Power Connector	• Connect the included power cords to these connectors
2.Serial Port	• This port is for external UPS device
3.eSATA Port	• eSATA port for high-speed storage expansion
4.USB Port	• USB 2.0 port for compatible USB devices, such as USB disks, and USB printers

5.USB Port	• USB 3.0 port for compatible USB devices.
6.WAN/LAN1 Port	• WAN/LAN1 port for connecting to an Ethernet network through a switch or router
7.LAN2 Port	• LAN2 port for connecting to an Ethernet network through a switch or router
8.LAN3 Port	• LAN3 port for HA connecting.

N12000V/N12000PRO:

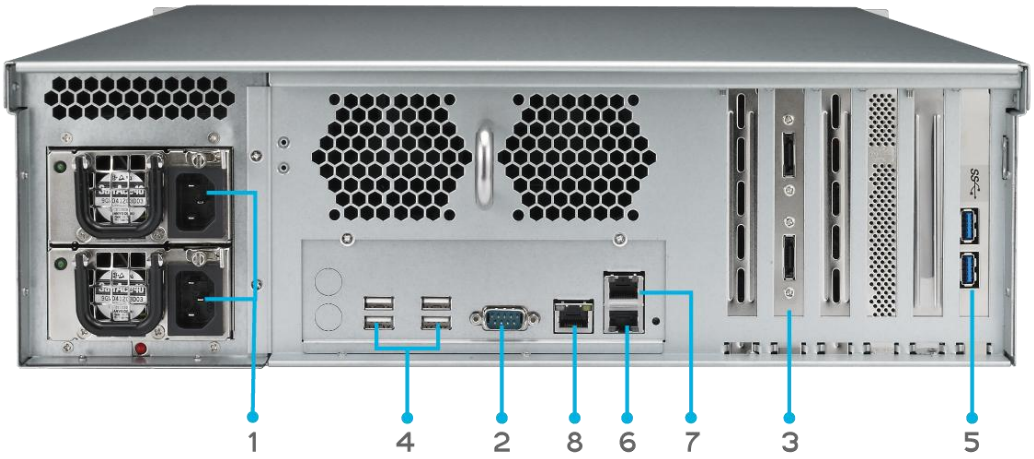
N12000V/N12000PRO rear panel features ports and connectors.



Back Panel	
Item	**Description**
1.Power Connector	• Connect the included power cords to these connectors
2.Serial Port	• This port is for external UPS device
3.eSATA Port	• eSATA port for high-speed storage expansion
4.USB Port	• USB 2.0 port for compatible USB devices, such as USB disks, and USB printers
5.USB Port	• USB 3.0 port for compatible USB devices.
6.WAN/LAN1 Port	• WAN/LAN1 port for connecting to an Ethernet network through a switch or router
7.LAN2 Port	• LAN2 port for connecting to an Ethernet network through a switch or router
8.LAN3 Port	• LAN3 port for HA connecting.
9.HDMI Port	• For Video/Audio out
10. Mic input	• Microphone input
11. Line out	• For Audio out
12.Line in	• For Audio in

N16000:

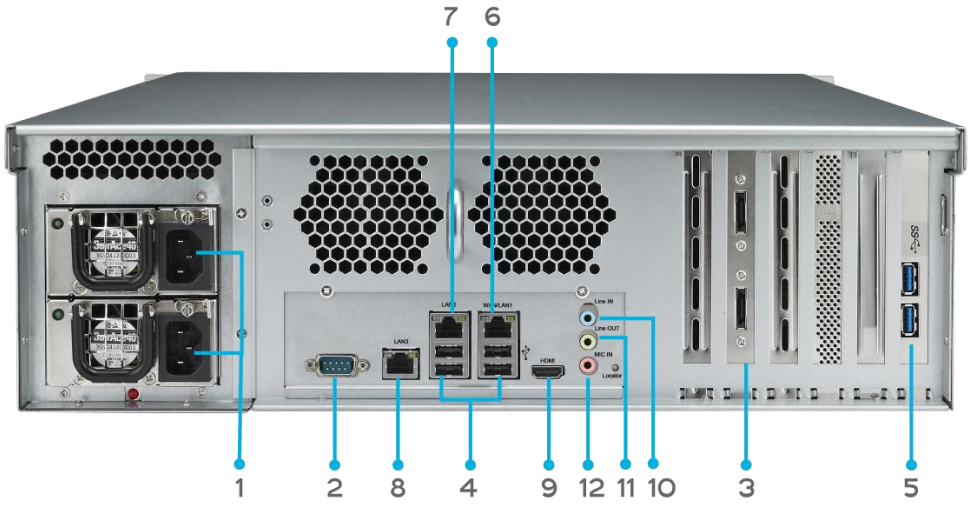
The N16000 rear panel features ports and connectors.



Back Panel	
Item	**Description**
1.Power Connector	• Connect the included power cords to these connectors
2.Serial Port	• This port is for external UPS device
3.eSATA Port	• eSATA port for high-speed storage expansion
4.USB Port	• USB 2.0 port for compatible USB devices, such as USB disks, and USB printers
5.USB Port	• USB 3.0 port for compatible USB devices.
6.WAN/LAN1 Port	• WAN/LAN1 port for connecting to an Ethernet network through a switch or router
7.LAN2 Port	• LAN2 port for connecting to an Ethernet network through a switch or router
8.LAN3 Port	• LAN3 port for HA connecting.

N16000V/N16000PRO:

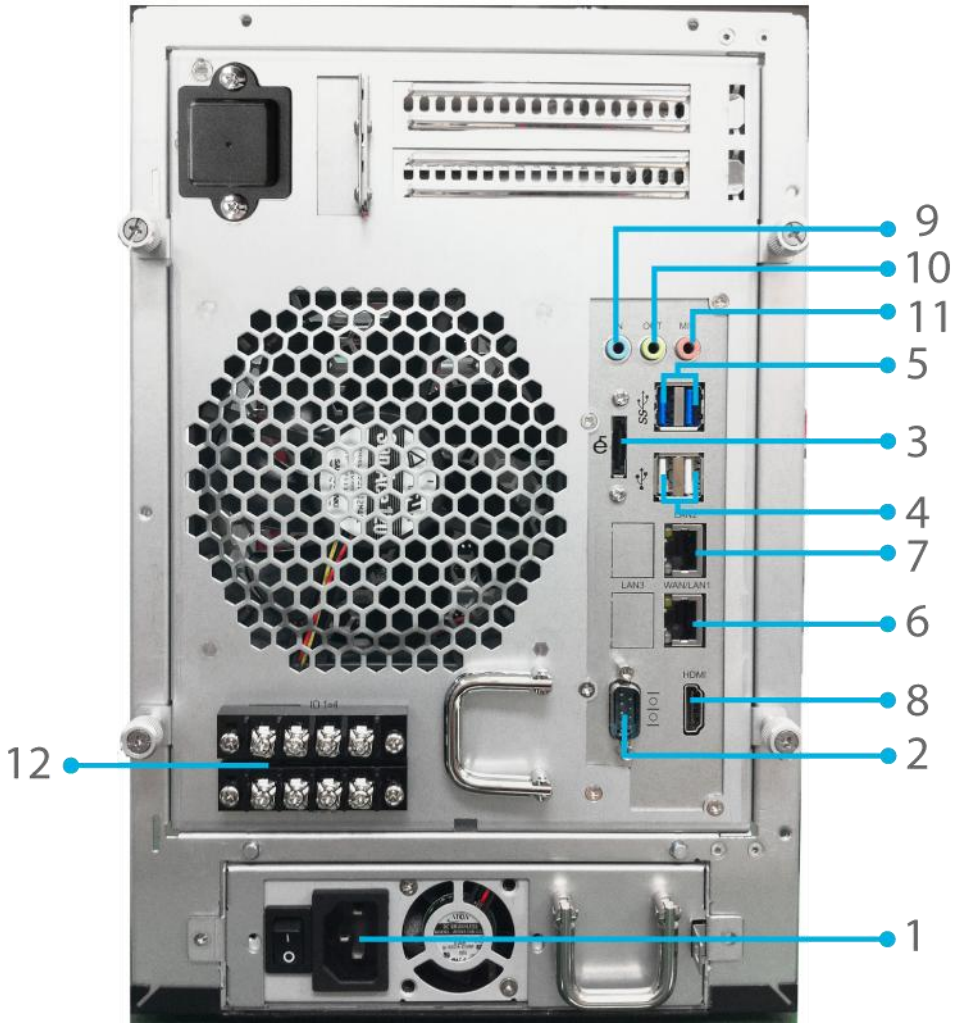
N16000V/N16000PRO rear panel features ports and connectors.



Back Panel	
Item	**Description**
1.Power Connector	• Connect the included power cords to these connectors
2.Serial Port	• This port is for external UPS device
3.eSATA Port	• eSATA port for high-speed storage expansion
4.USB Port	• USB 2.0 port for compatible USB devices, such as USB disks, and USB printers
5.USB Port	• USB 3.0 port for compatible USB devices.
6.WAN/LAN1 Port	• WAN/LAN1 port for connecting to an Ethernet network through a switch or router
7.LAN2 Port	• LAN2 port for connecting to an Ethernet network through a switch or router
8.LAN3 Port	• LAN3 port for HA connecting.
9.HDMI Port	• For Video/Audio out
10.Line in	• For Audio in
11. Line out	• For Audio out
12. Mic input	• Microphone input

N6850:

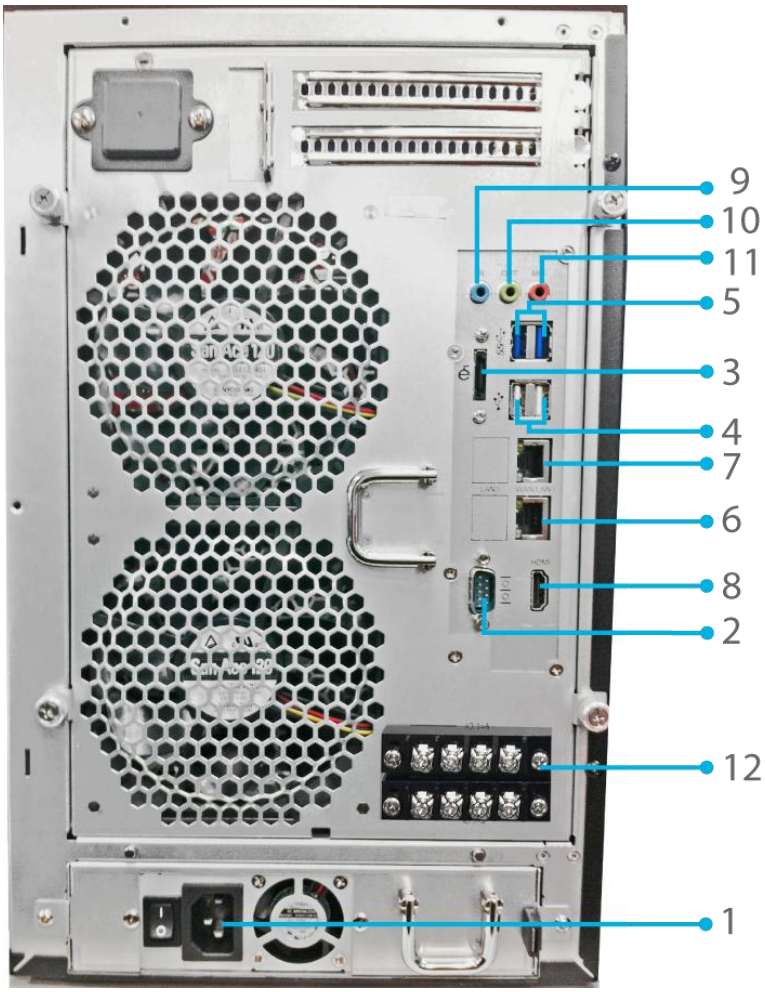
The N6850 rear panel features ports and connectors.



Back Panel	
Item	**Description**
1.Power Connector	• Connect the included power cords to these connectors
2.Serial Port	• This port is for external UPS device
3.eSATA Port	• eSATA port for high-speed storage expansion
4.USB Port	• USB 2.0 port for compatible USB devices, such as USB disks, and USB printers
5.USB Port	• USB 3.0 port for compatible USB devices.
6.WAN/LAN1 Port	• WAN/LAN1 port for connecting to an Ethernet network through a switch or router
7.LAN2 Port	• LAN2 port for connecting to an Ethernet network through a switch or router
8.HDMI Port	• For Video/Audio out
9.Line in	• For Audio in
10. Line out	• For Audio out
11. Mic input	• Microphone input
12. User GPIO	• Could define each GPIO (0~7) and implement its own functionality.

N8850:

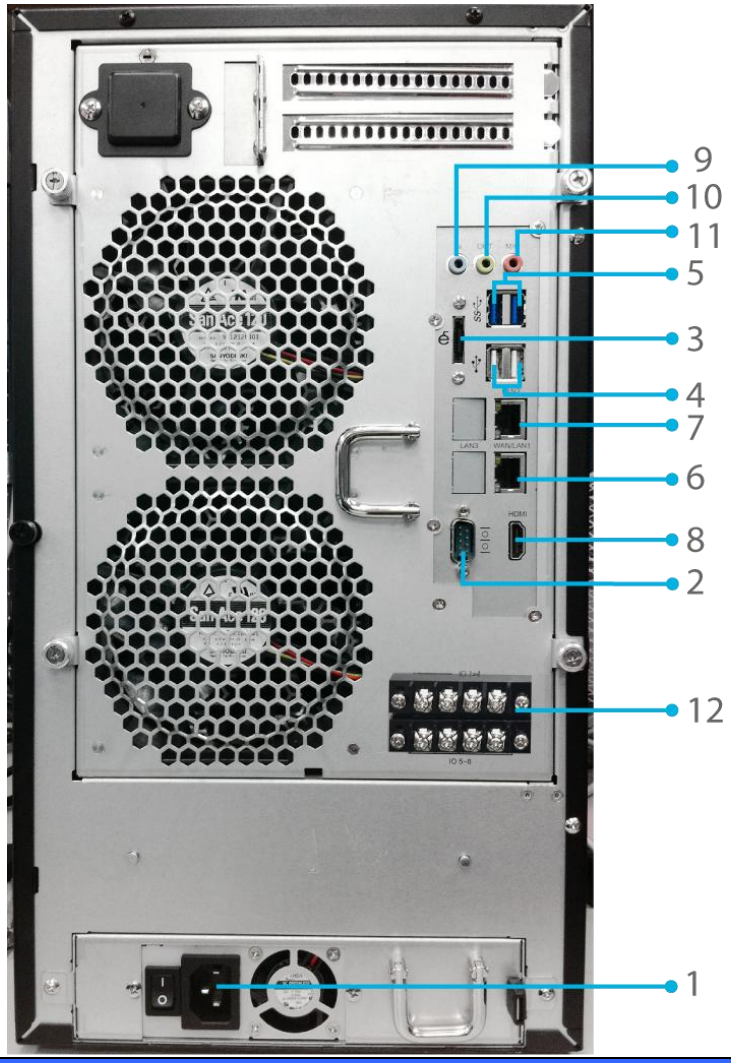
The N8850 rear panel features ports and connectors.



Back Panel	
Item	**Description**
1.Power Connector	• Connect the included power cords to these connectors
2.Serial Port	• This port is for external UPS device
3.eSATA Port	• eSATA port for high-speed storage expansion
4.USB Port	• USB 2.0 port for compatible USB devices, such as USB disks, and USB printers
5.USB Port	• USB 3.0 port for compatible USB devices.
6.WAN/LAN1 Port	• WAN/LAN1 port for connecting to an Ethernet network through a switch or router
7.LAN2 Port	• LAN2 port for connecting to an Ethernet network through a switch or router
8.HDMI Port	• For Video/Audio out
9.Line in	• For Audio in
10. Line out	• For Audio out
11. Mic input	• Microphone input
12. User GPIO	• Could define each GPIO (0~7) and implement its own functionality.

N10850:

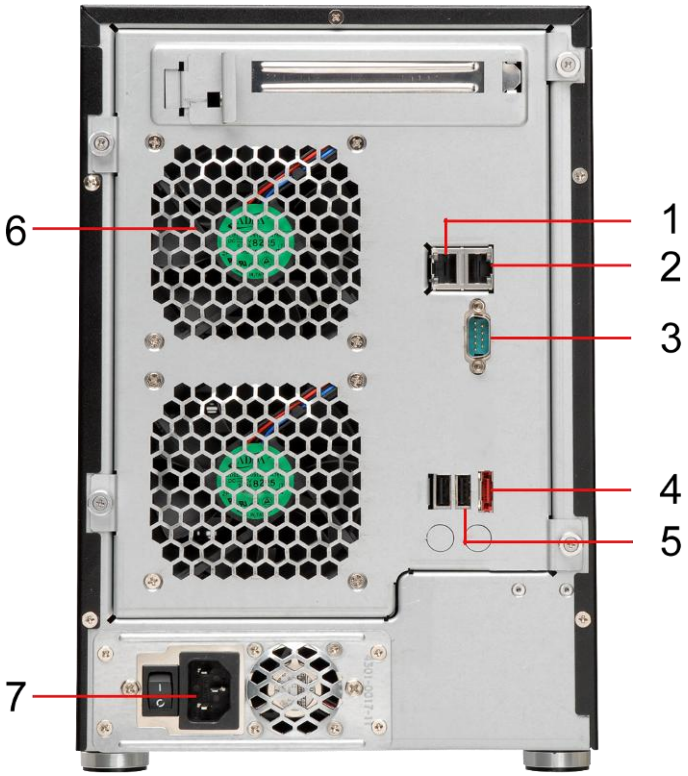
The N10850 rear panel features ports and connectors.



Back Panel	
Item	**Description**
1.Power Connector	• Connect the included power cords to these connectors
2.Serial Port	• This port is for external UPS device
3.eSATA Port	• eSATA port for high-speed storage expansion
4.USB Port	• USB 2.0 port for compatible USB devices, such as USB disks, and USB printers
5.USB Port	• USB 3.0 port for compatible USB devices.
6.WAN/LAN1 Port	• WAN/LAN1 port for connecting to an Ethernet network through a switch or router
7.LAN2 Port	• LAN2 port for connecting to an Ethernet network through a switch or router
8.HDMI Port	• For Video/Audio out
9.Line in	• For Audio in
10.Line out	• For Audio out
11.Mic input	• Microphone input
12. User GPIO	• Could define each GPIO (0~7) and implement its own functionality.

N7700PRO V2:

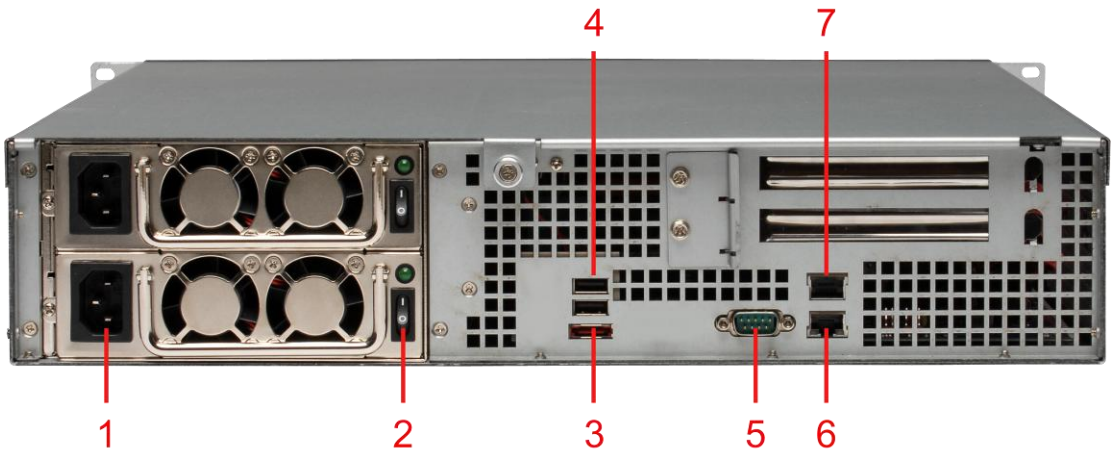
The N7700PRO V2 rear panel features ports and connectors.



Back Panel	
Item	**Description**
1.LAN2 Port	• LAN2 port for connecting to a local Ethernet network through a switch or router.
2.WAN/LAN1 Port	• WAN/LAN1 port for connecting to an Ethernet network through a switch or router.
3.Serial Port	• This port is for an external UPS device.
4.eSATA Port	• eSATA port for high-speed storage expansion.
5.USB Port	• USB 2.0 port for compatible USB devices, such as USB disks, and USB printers.
6.System Fan	• System fan that exhausts heat from the unit.
7.Power Connector	• Connect the included power cord to this connector.

N8800PRO V2:

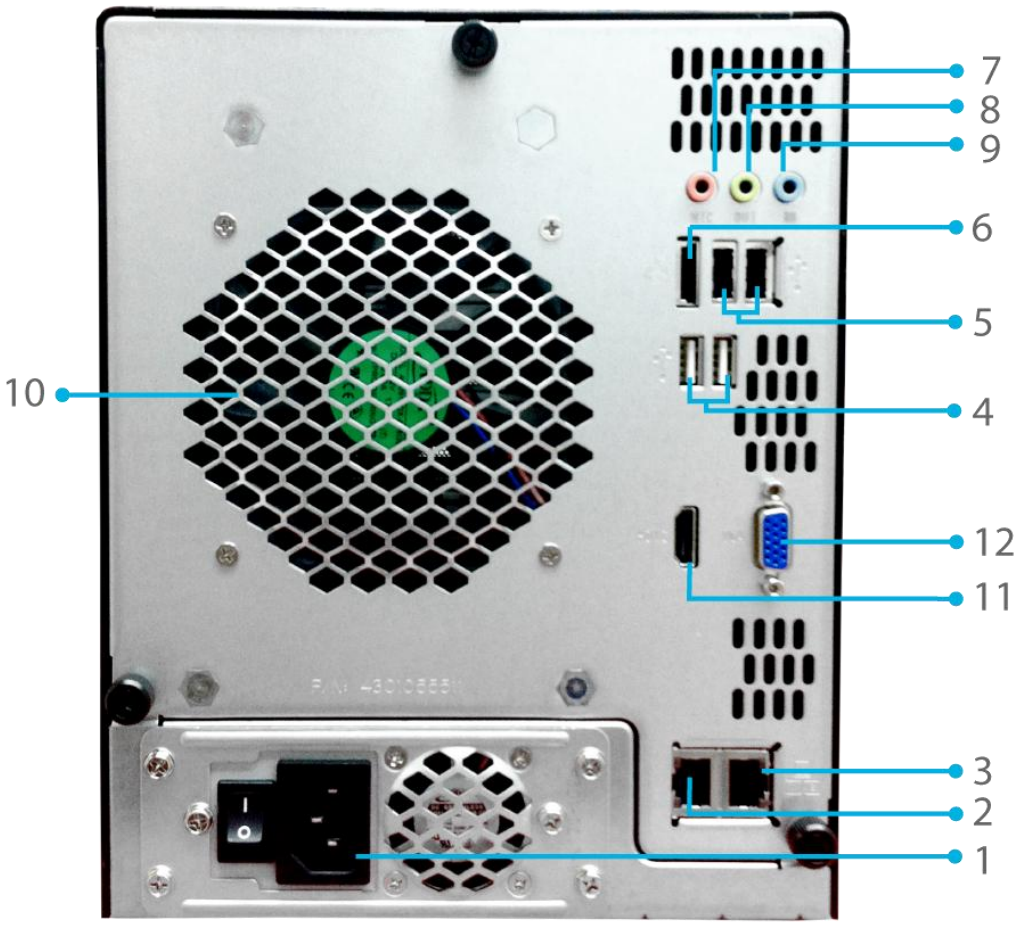
The N8800PRO V2 rear panel features ports and connectors.



Back Panel	
Item	**Description**
1.Power Connector	• Connect the included power cords to these connectors
2.Power Switch	• Switch for power supply
3.eSATA Port	• eSATA port for high-speed storage expansion
4.USB Port	• USB 2.0 port for compatible USB devices, such as USB disks, and USB printers
5.Serial Port	• This port is for external UPS device
6.WAN/LAN1 Port	• WAN/LAN1 port for connecting to an Ethernet network through a switch or router
7.LAN2 Port	• WAN/LAN1 port for connecting to an Ethernet network through a switch or router

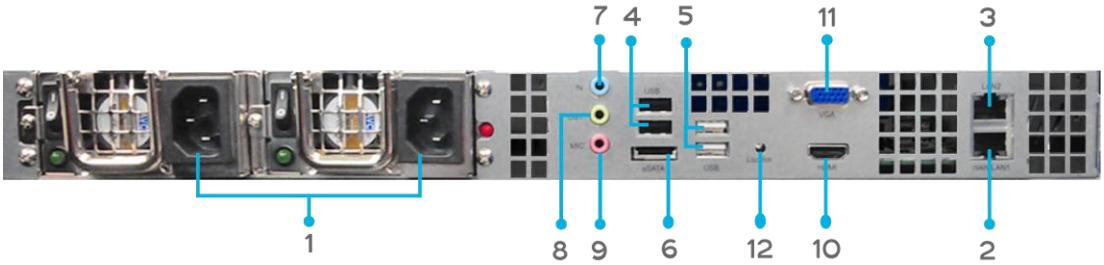
N5550:

The N5550 rear panel features ports and connectors.



Back Panel	
Item	**Description**
1.Power Connector	• Connect the included power cords to these connectors
2. WAN/LAN1 Port	• WAN/LAN1 port for connecting to an Ethernet network through a switch or router
3. LAN2 Port	• LAN2 port for connecting to an Ethernet network through a switch or router
4.USB Port	• USB 2.0 port for compatible USB devices, such as USB disks, and USB printers
5.USB Port	• USB 2.0 port for compatible USB devices.
6.eSATA Port	• eSATA port for high-speed storage expansion
7.Line in	• For Audio in
8. Line out	• For Audio out
9. Mic input	• Microphone input
10.System Fan	• System fan that exhausts heat from the unit.
11.HDMI Port	• For Video/Audio out
12.VGA Port	• For Video out

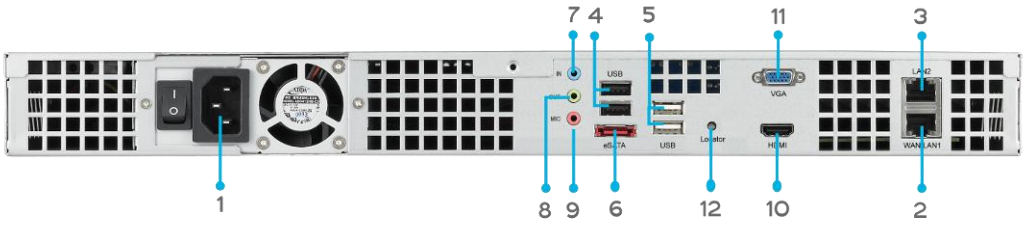
N4510U-R:



Back Panel	
Item	**Description**
1.Power Connector	• Connect the included power cords to these connectors
2. WAN/LAN1 Port	• WAN/LAN1 port for connecting to an Ethernet network through a switch or router
3. LAN2 Port	• LAN2 port for connecting to an Ethernet network through a switch or router
4.USB Port	• USB 2.0 port for compatible USB devices, such as USB disks, and USB printers
5.USB Port	• USB 2.0 port for compatible USB devices.
6.eSATA Port	• eSATA port for high-speed storage expansion
7.Line in	• For Audio in
8. Line out	• For Audio out
9. Mic input	• Microphone input
10.HDMI Port	• For Video/Audio out
11.VGA Port	• For Video out
12. Locator LED	• Identifies each NAS within a rack mount configuration.

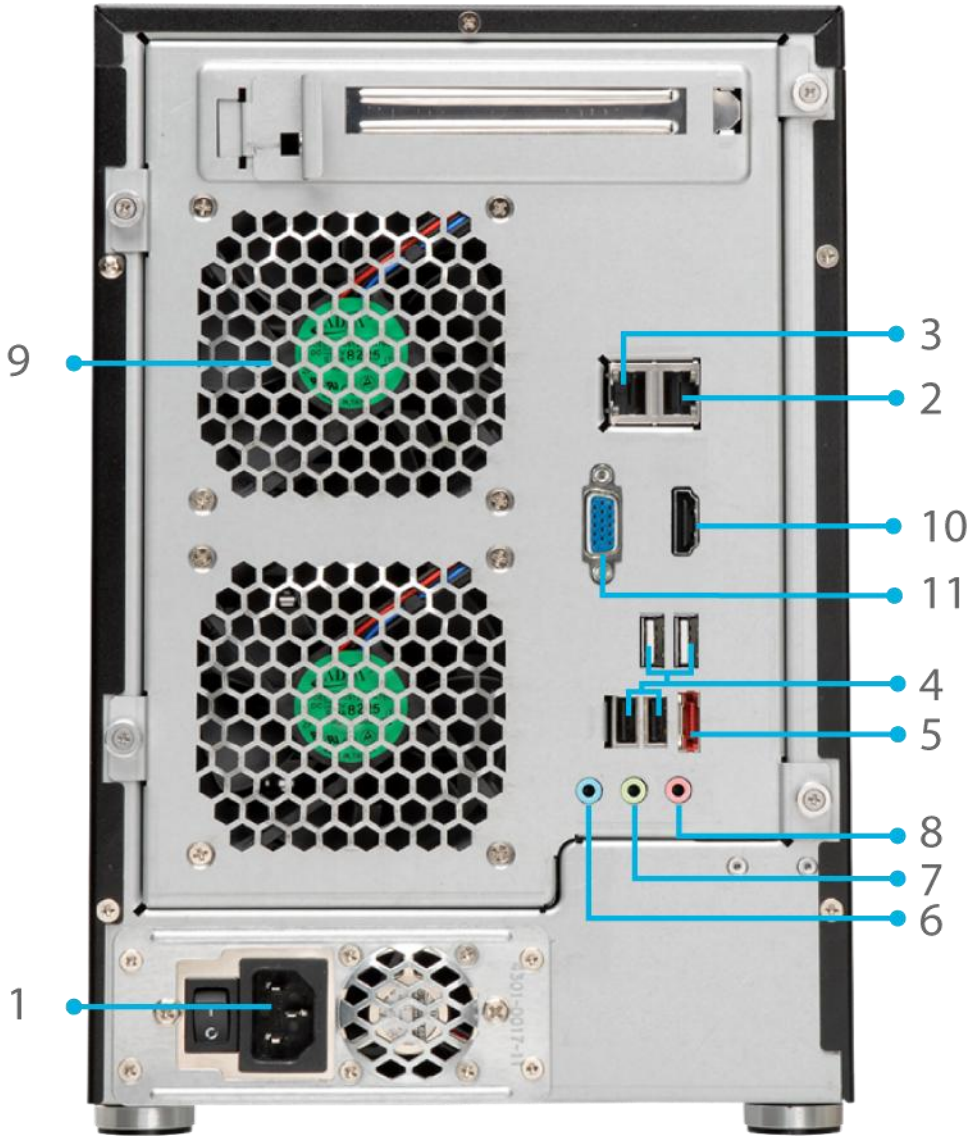
N4510U-S:

The rear panel of the N4510U-S is similar to the N4510U-R, but with a single power connector:



N7510:

The N7510 rear panel features ports and connectors.



Back Panel	
Item	**Description**
1.Power Connector	• Connect the included power cords to these connectors
2. WAN/LAN1 Port	• WAN/LAN1 port for connecting to an Ethernet network through a switch or router
3. LAN2 Port	• LAN2 port for connecting to an Ethernet network through a switch or router
4.USB Port	• USB 2.0 port for compatible USB devices, such as USB disks, and USB printers
5.eSATA Port	• eSATA port for high-speed storage expansion
6.Line in	• For Audio in
7. Line out	• For Audio out
8. Mic input	• Microphone input
9.System Fan	• System fan that exhausts heat from the unit.
10.HDMI Port	• For Video/Audio out
11.VGA Port	• For Video out

Chapter 2: Hardware Installation

Overview

Your Thecus IP storage is designed for easy installation. To help you get started, the following chapter will help you quickly get your Thecus IP storage up and running. Please read it carefully to prevent damaging your unit during installation.

Before You Begin

Before you begin, be sure to take the following precautions:

1. Read and understand the ***Safety Warnings*** outlined in the beginning of the manual.

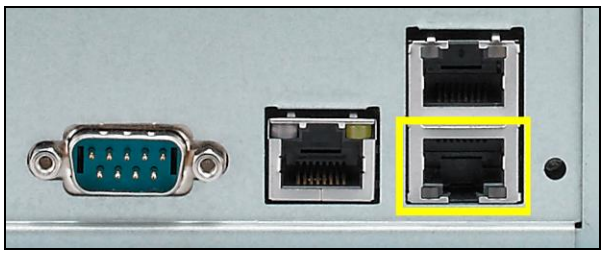
2. If possible, wear an anti-static wrist strap during installation to prevent static discharge from damaging the sensitive electronic components on the Thecus IP storage.

3. Be careful not to use magnetized screwdrivers around the Thecus IP storage's electronic components.

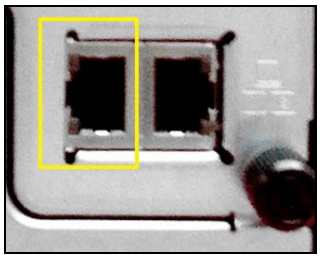
Cable Connections

To connect the Thecus IP storage product to your network, follow the steps below:

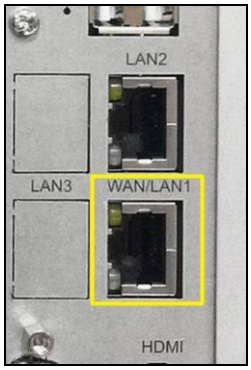
1. Connect an Ethernet cable from your network to the WAN/LAN1 port on the back panel of the Thecus IP storage.



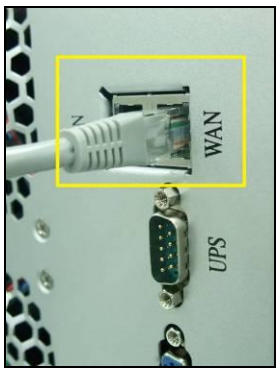
▲ *N12000 series/N16000 series/N8900 series WAN/LAN1 port*



▲*N5550 WAN/LAN1 port*

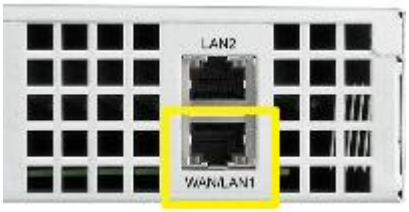


▲ *N6850/N8850/N10850 WAN/LAN1 port*



▲ *N7700PRO V2 WAN/LAN1 port*

▲ *N8800PRO V2 WAN/LAN1 port*

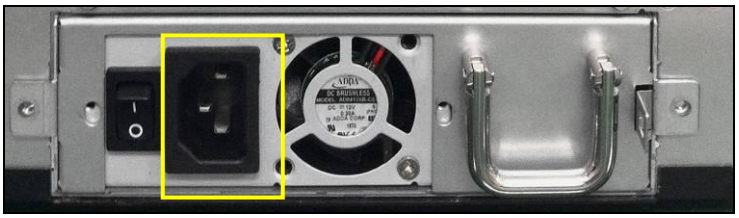


▲ *N4510U WAN/LAN1 port*

▲ *N7510 WAN/LAN1 port*

2. Connect the provided power cord into the universal power socket on the back panel. Plug the other end of the cord into a surge protector socket.

▲ *N12000 series/N16000 series/N8900 series power socket*



▲ *N6850/N8850/N10850 power socket*

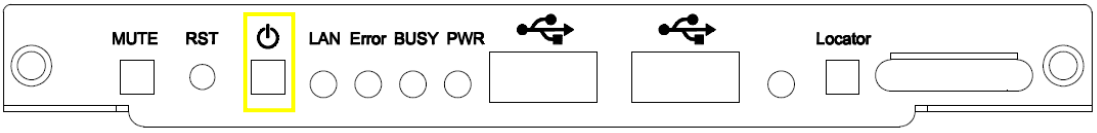
▲ *N7700PRO V2 /N7510 power socket*

▲ *N8800PRO V2 power socket*

▲*N5550 power socket*

▲*N4510U power socket*

3. Press the power button on the Front Panel to boot up the Thecus IP storage.



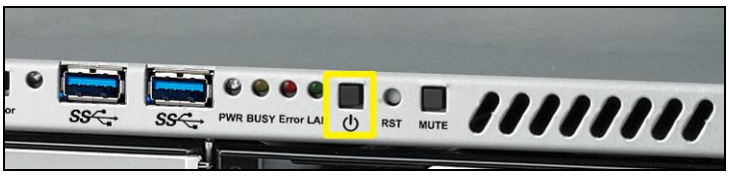
▲ *N12000 series/N16000 series/N8900 series power button*

▲*N6850/N8850/N10850 power button*

▲*N5550 power button*

▲ *N7700PRO V2/ N7510 power button*

▲ *N8800PRO V2 power button*



▲ *N4510U power button*

Chapter 3: First Time Setup

Overview

Once the hardware is installed, physically connected to your network, and powered on, you can configure the Thecus IP storage so that it is accessible to your network users. There are two ways to set up your Thecus IP storage: using the **Thecus Setup Wizard** or the **LCD display**. Follow the steps below for initial software setup.

Thecus Setup Wizard

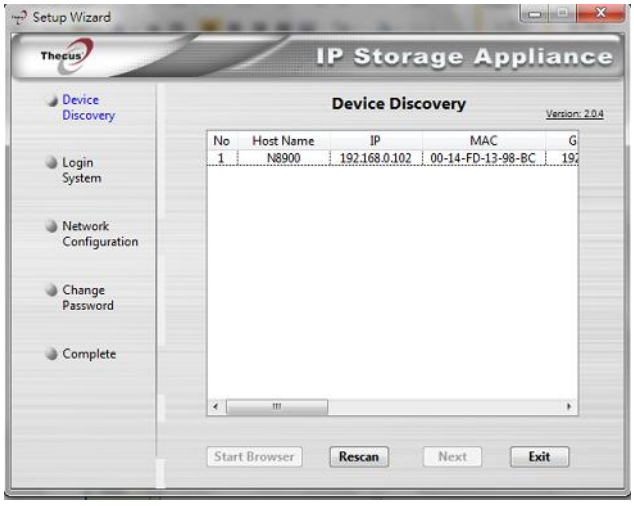
The handy Thecus Setup Wizard makes configuring Thecus IP storage a snap. To configure the Thecus IP storage using the Setup Wizard, perform the following steps:

1. Insert the installation CD into your CD-ROM drive (the host PC must be connected to the network).

2. The Setup Wizard should launch automatically. If not, please browse your CD-ROM drive and double click on **Setup.exe.**

NOTE For MAC OS X users, double click on Thecus Setup Wizard .dmg file.

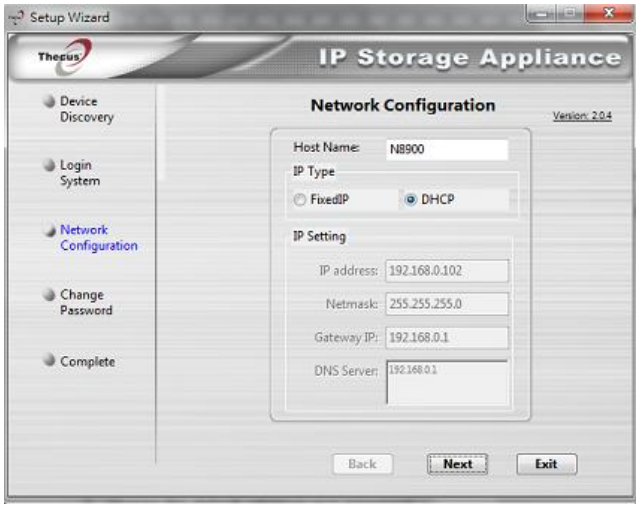
3. The Setup Wizard will start and automatically detect all Thecus storage devices on your network. If none are found, please check your connection and refer to **Chapter 7: Troubleshooting** for assistance.



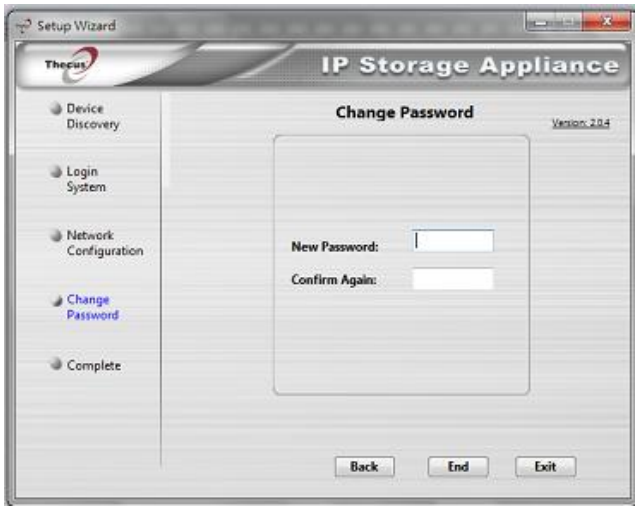
4. Select the Thecus IP storage that you like to configure.

5. Login with the administrator account and password. The default account and password are both "`admin`".

6. Name your Thecus IP storage and configure the network IP address. If your switch or router is configured as a DHCP Server, configuring the Thecus IP storage to automatically obtain an IP address is recommended. You may also use a static IP address and enter the DNS Server address manually.



7. Change the default administrator password.



8. Finished! Access the Thecus IP storage Web Administrator Interface by pressing the ***Start Browser*** button. You can also configure another Thecus IP storage at this point by clicking the ***Setup Other Device*** button. Press ***Exit*** to exit the wizard.

NOTE

The Thecus Setup Wizard is designed for installation on systems running Windows XP/2000/vista/7 or Mac OSX or later. Users with other operating systems will need to install the Thecus Setup Wizard on a host machine with one of these operating systems before using the unit.

LCD Operation (N7700PRO V2/N8800PRO V2/N5550/N4510U/N7510)

The mentioned models above are equipped with an LCD on the front for easy status display and setup. There are four buttons on the front panel to control the LCD functions.

LCD Controls

Use the **Up** (▲), **Down** (▼), **Enter** (↵) and **Escape** (**ESC**) keys to select various configuration settings and menu options for Thecus IP storage configuration.

The following table illustrates the keys on the front control panel:

LCD Controls		
Icon	**Function**	**Description**
▲	Up Button	Select the previous configuration settings option.
▼	Down Button	USB copy confirmation display.
↵	Enter	Enter the selected menu option, sub-menu, or parameter setting.
ESC	Escape	Escape and return to the previous menu.

There are two modes of operation for the LCD: **Display Mode** and **Management Mode**.

Display Mode

During normal operation, the LCD will be in **Display Mode**.

Display Mode	
Item	**Description**
Host Name	Current host name of the system.
WAN/LAN1	Current WAN/LAN1 IP setting.
LAN2	Current LAN2 IP setting.
Link Aggregation	Current Link Aggregation status
System Fan1	Current system fan1 status.
System Fan2	Current system fan2 status.
CPU Fan	Current CPU fan status
2009/05/22 12:00	Current system time.
Disk Info	Current status of disk slot has been installed
RAID	Current RAID status.

The Thecus IP storage will rotate these messages every one-two seconds on the LCD display.

USB Copy

The USB Copy function enables you to copy files stored on USB devices such as USB disks and digital cameras to the Thecus IP storage by press button. To use USB copy, follow the steps below:

1. Plug your USB device into an available USB port on the Front end.
2. In **Display Mode**, press the **Down Button** (▼).
3. The LCD will display "`USB Copy?`"
4. Press **Enter** (↵) and the Thecus IP storage will start copying USB disks connected to the front USB port.
5. All of data will be copied into system folder named "USB copy".

Management Mode

During setup and configuration, the LCD will be in **Management Mode**.

To enter into Management Mode, press **Enter (↵)** and an "*Enter Password*" prompt will show on the LCD.

At this time, the administrator has to enter the correct LCD password. System will check whether the correct LCD password has been entered. The default LCD password is " `0000` ". If correct password is entered, you will enter into the **Management Mode** menu.

Management Mode	
Item	**Description**
WAN/LAN1 Setting	IP address and netmask of your WAN/LAN1 ports.
LAN2 Setting	IP address and netmask of your LAN2 ports.
Link Agg. Setting	Select **Load Balance, 802.3ad** or **Failover**.
Change Admin Passwd	Change administrator's password for LCD operation.
Reset to Default	Reset system to factory defaults.
Exit	Exit **Management Mode** and return to **Display Mode**.

NOTE

You can also change your LCD password using the Web Administration Interface by navigating to **System Management > Administrator Password**. For more on the Web Administration Interface, see **Chapter 4: System Management**.

OLED Operation(Does not apply to the N7700PRO V2/N8800PRO V2/N5550/N4510U/N7510)

OLED Operation

The Thecus IP storage is equipped with an OLED on the front for easy status display and setup. There are four buttons on the front panel to control the OLED functions.

OLED Controls

Use the **Up** (▲), **Down** (▼), **Enter** (↵) and **Escape** (**ESC**) keys to select various configuration settings and menu options for Thecus IP storage configuration.

The following table illustrates the keys on the front control panel:

OLED Controls		
Icon	**Function**	**Description**
▲	Up Button	Select the previous configuration settings option.
▼	Down Button	USB copy confirmation display.
↵	Enter	Enter the selected menu option, sub-menu, or parameter setting.
ESC	Escape	Escape and return to the previous menu.

There are two modes of operation for the OLED: **Display Mode** and **Management Mode**.

Display Mode

During normal operation, the OLED will be in **Display Mode**.

Display Mode	
Item	**Description**
Host Name	Current host name of the system.
WAN/LAN1	Current WAN/LAN1 IP setting.
LAN2	Current LAN2 IP setting.
Link Aggregation	Current Link Aggregation status
System Fan	Current system fan status.
CPU Fan	Current CPU fan status
2009/05/22 12:00	Current system time.
RAID	Current RAID status.

The Thecus IP storage will rotate these messages every one-two seconds on the OLED display.

USB Copy

The USB Copy function enables you to copy files stored on USB devices such as USB disks and digital cameras to the Thecus IP storage with a press of a button. To use USB copy, follow the steps below:

1. Plug your USB device into an available USB port on the Front Panel.
2. In **Display Mode**, press the **Enter** (↵).

3. The LCD will display "**USB Copy?**"

4. Press **Enter** (↵) and the Thecus IP storage will start copying USB disks connected to the front USB port. The LCD will display the USB copy progress and results.

Typical Setup Procedure

From the Web Administration Interface, you can begin to setup your Thecus IP storage for use on your network. Setting up the Thecus IP storage typically follows the five steps outlined below.

For more on how to use the Web Administration Interface, see
Chapter 4: Web Administration Interface.

Step 1: Network Setup

From the Web Administration Interface, you can configure the network settings of the Thecus IP storage for your network. You can access the **Network** menu from the menu bar.
For details on how to configure your network settings, refer to
Chapter 4: System Network .

Step 2: RAID Creation

Next, administrators can configure their preferred RAID setting and build their RAID volume. You can access RAID settings from the menu bar of the Web Administration Interface by navigating to **Storage Management > RAID Management.**

For more information on configuring RAID, see
Chapter 4: Storage > RAID Management.

Don't know which RAID level to use? Find out more about the different RAID levels from **Appendix B: RAID Basics**.

Step 3: Create Local Users or Setup Authentication

Once the RAID is ready, you can begin to create local users for Thecus IP storage, or choose to setup authentication protocols such as Active Directory (AD).

For more on managing users, go to **Chapter 4: User and Group Authentication**.

For more information on configuring Active Directory, see
Chapter 4: User and Group Authentication > ADS Support.

For information about the benefits of Active Directory, see **Appendix D: Active Directory Basics**.

Step 4: Create Folders and Set Up ACLs

Once users are introduced into your network, you can begin to create various folders on the Thecus IP storage and control user access to each using Folder Access Control Lists.

More information on managing folders, see
Chapter 4: Storage Management > Share Folder .

To find out about configuring Folder Access Control Lists, see **Chapter 4: Storage Management > Share Folder> Folder Access Control List (ACL)**.

Step 5: Start Services

Finally, you can start to setup the different services of Thecus IP storage for the users on your network. You can find out more about each of these services by clicking below:

SMB/CIFS

Apple File Protocol (AFP)

Network File System (NFS)

File Transfer Protocol (FTP)

iTunes Server

Printer Server

Chapter 4: System Administration

Overview

The Thecus IP storage provides an easily accessible **Web Administration Interface**. With it, you can configure and monitor the Thecus IP storage anywhere on the network.

Web Administration Interface

Make sure your network is connected to the Internet. To access Thecus IP storage **Web Administration Interface**:

1. Type the Thecus IP storage IP address into your browser. (Default IP address is `http://192.168.1.100`)

NOTE

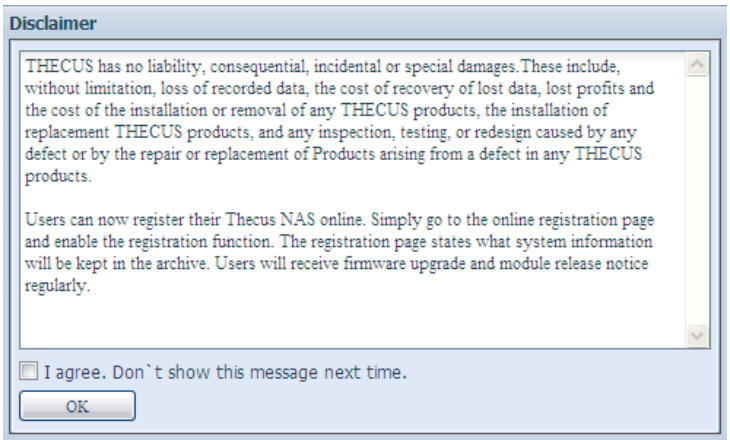
Your computer's network IP address must be on the same subnet as the Thecus IP storage. If the Thecus IP storage has default IP address of 192.168.1.100, your managing PC IP address must be 192.168.1.x, where x is a number between 1 and 254, but not *100*.

2. Login to the system using the administrator user name and password. The factory defaults are:

   User Name: `admin`
   Password: `admin`

※ If you changed your password in the setup wizard, use the new password.

Once you are logged in as an administrator, the disclaimer page will appear as below. Please click the check box if you do not want to have this page displayed during the next login.


Disclaimer
THECUS has no liability, consequential, incidental or special damages.These include, without limitation, loss of recorded data, the cost of recovery of lost data, lost profits and the cost of the installation or removal of any THECUS products, the installation of replacement THECUS products, and any inspection, testing, or redesign caused by any defect or by the repair or replacement of Products arising from a defect in any THECUS products.
Users can now register their Thecus NAS online. Simply go to the online registration page and enable the registration function. The registration page states what system information will be kept in the archive. Users will receive firmware upgrade and module release notice regularly.
I agree. Don`t show this message next time.
OK

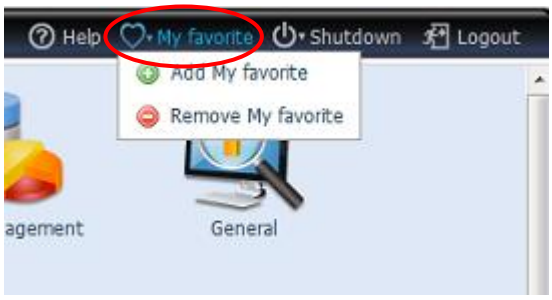
Following the disclaimer page, you will see the **Web Administration Interface**. From here, you can configure and monitor virtually every aspect of the Thecus IP storage from anywhere on the network.

My Favorite

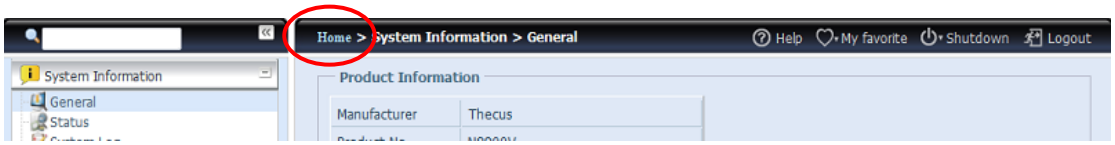
The user interface with "My Favorite" shortcut allows the user to designate often used items and have them display on the main screen area. The figure below displays system favorite functions.

Administrators can add or remove favorite functions to My Favorites by right clicking the mouse on the menu tree.

Another way the administrators can add favorite functions is by clicking the "Add Favorite" icon in each function screen. See the figure below with the red circled icon.



To return to the favorite screen, simply click "Home" located at the left hand corner of the main screen.



Menu Bar

The **Menu Bar** is where you will find all of the information screens and system settings of Thecus IP storage. The various settings are placed in the following groups on the menu bar:

Menu Bar	
Item	**Description**
System Information	Current system status of the Thecus IP storage.
System Management	Various Thecus IP storage system settings and information.
System Network	Information and settings for network connections, as well as various services of the Thecus IP storage.
Storage	Information and settings for storage devices installed into the Thecus IP storage.
User and Group Authentication	Allows configuration of users and groups.
Network Service	
Application Server	Printer Server and iTunes Server set-up of the Thecus IP storage.
Module Management	System and user Module installation of the Thecus IP storage.
Backup	Category of Backup Features setup of the Thecus IP storage.

Moving your cursor over any of these items will display the dropdown menu selections for each group.

In the following sections, you will find detailed explanations of each function, and how to configure your Thecus IP storage.

Message Bar

You can get quick information about your system status by moving your mouse over these icons.

Message Bar		
Item	**Status**	**Description**
	RAID Information.	Display the status of created RAID volume. Click to go to RAID information page as short cut.
	Disks Information.	Display the status of disks installed in the system. Click to go to Disk information page as short cut.
	FAN.	Display system FAN Status. Click to go to System Status page as short cut.
	Network.	Green: Connection to the network is normal. Red: abnormal connection to the network
	Temperature	Display system temperature, click to go to System Status page as shot cut.

Logout

Click to logout Web Administration Interface.

Language Selection

The Thecus IP storage supports multiple Languages, including:

- English
- Japanese
- Traditional Chinese
- Simplified Chinese
- French
- German
- Italian
- Korean
- Spanish
- Russian
- Polish
- Portuguese

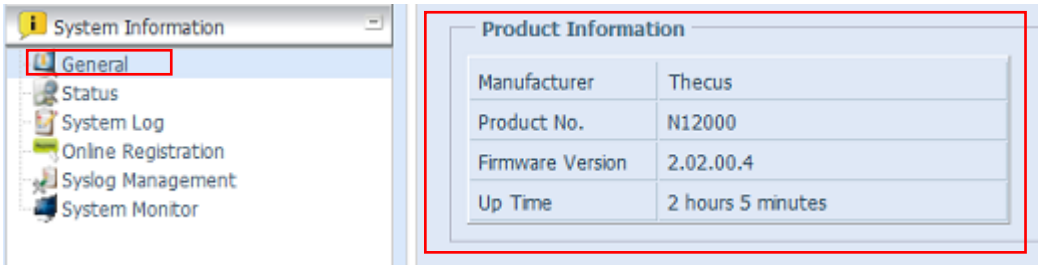
On the menu bar, click **Language** and the **selection** list appears. This user interface will switch to the selected language for Thecus IP storage.

System Information

Information provides viewing on current Product info, System Status, Service Status and Logs.
The menu bar allows you to see various aspects of the Thecus IP storage. From here, you can discover the status of the Thecus IP storage, and also other details.

System Information

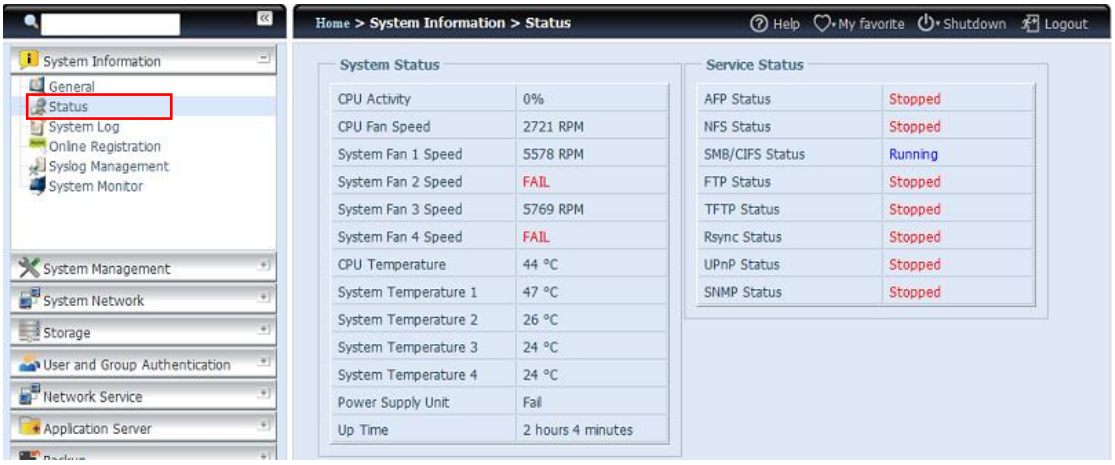
Once you login, you will first see the basic **system Information** screen providing **Manufacturer**, **Product No.**, **Firmware Version**, and **System Up Time** information.



System Information	
Item	**Description**
Manufacturer	Displays the name of the system manufacturer.
Product No.	Shows the model number of the system.
Firmware version	Shows the current firmware version.
Up time	Displays the total run time of the system.

System/Service Status (Refer Chapter 7 for FW v2.03.01 and after)

From the **System Information** menu, choose the ***Status*** item, **System Status** and **Service Status** screens appear. These screens provide basic system and service status information.



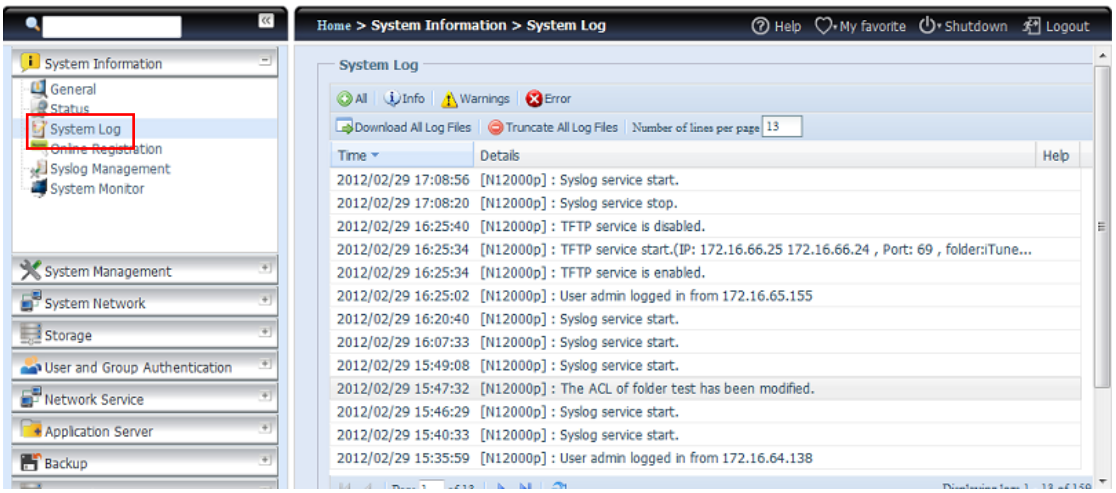
System Status	
Item	**Description**
CPU Activity	Displays current CPU workload of the Thecus IP storage.
CPU Fan Speed	Displays current CPU fan status.

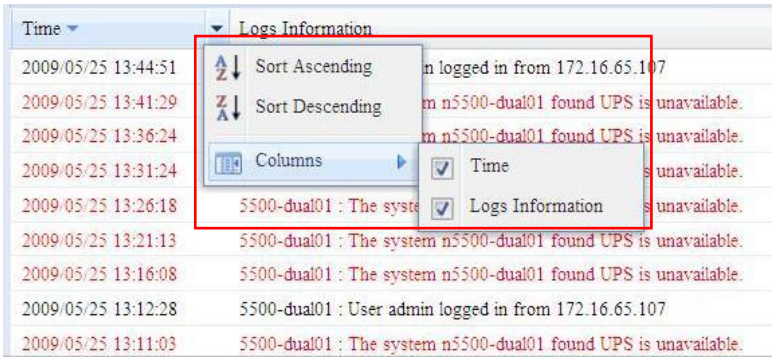
System Fan 1 Speed	Displays current System fan (left 1) status
System Fan 2 Speed	Displays current System fan (left 2) status
System Fan 3 Speed	Displays current System fan (left 3) status (Depend on model)
System Fan 4 Speed	Displays current System fan (left 4) status (Depend on model)
CPU Temperature	Displays current CPU Temperature.
System Temperature 1	Displays current System temperature in position 1
System Temperature 2	Displays current System temperature in position 2
System Temperature 3	Displays current System temperature in position 3
System Temperature 4	Displays current System temperature in position 4
System Fan Speed	Displays the current status of the system fan.
Up Time	Shows how long the system has been up and running.

Service Status	
Item	**Description**
AFP Status	The status of the Apple Filing Protocol server.
NFS Status	The status of the Network File Service Server.
SMB/CIFS Status	The status of the SMB/CIFS server.
FTP Status	The status of the FTP server.
TFTP Status	The status of the TFTP server.
Rsync Status	The status of the Rsync server.
UPnP Status	The status of the UPnP service.
SNMP	The status of the SNMP service.

Logs

From the **System Information** menu, choose the **System Logs** item and the **System Logs** screen appears. This screen shows a history of system usage and important events such as disk status, network information, and system booting. See the following table for a detailed description of each item:


Home > System Information > System Log
Help
My favorite
Shutdown
Logout
System Information
General
Status
System Log
Online Registration
Syslog Management
System Monitor
System Management
System Network
Storage
User and Group Authentication
Network Service
Application Server
Backup
System Log
All
Info
Warnings
Error
Download All Log Files
Truncate All Log Files
Number of lines per page 13
Time
Details
Help
2012/02/29 17:08:56 [N12000p] : Syslog service start.
2012/02/29 17:08:20 [N12000p] : Syslog service stop.
2012/02/29 16:25:40 [N12000p] : TFTP service is disabled.
2012/02/29 16:25:34 [N12000p] : TFTP service start.(IP: 172.16.66.25 172.16.66.24 , Port: 69 , folder:iTune...
2012/02/29 16:25:34 [N12000p] : TFTP service is enabled.
2012/02/29 16:25:02 [N12000p] : User admin logged in from 172.16.65.155
2012/02/29 16:20:40 [N12000p] : Syslog service start.
2012/02/29 16:07:33 [N12000p] : Syslog service start.
2012/02/29 15:49:08 [N12000p] : Syslog service start.
2012/02/29 15:47:32 [N12000p] : The ACL of folder test has been modified.
2012/02/29 15:46:29 [N12000p] : Syslog service start.
2012/02/29 15:40:33 [N12000p] : Syslog service start.
2012/02/29 15:35:59 [N12000p] : User admin logged in from 172.16.64.138

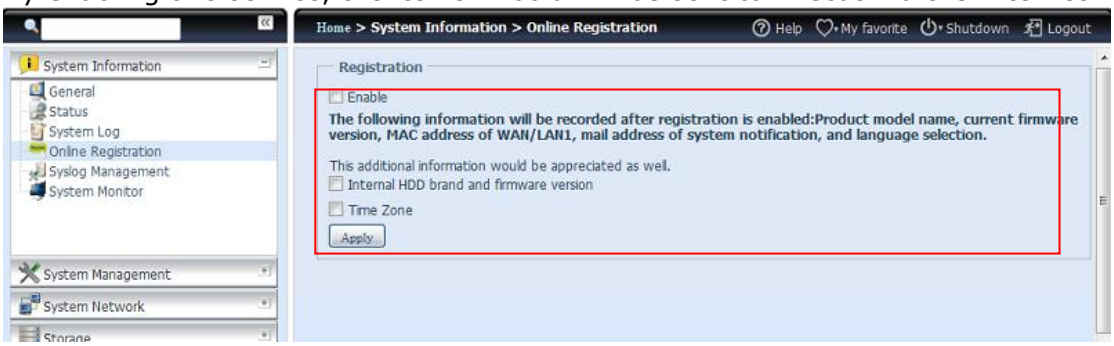


See the following table for a detailed description of each item:

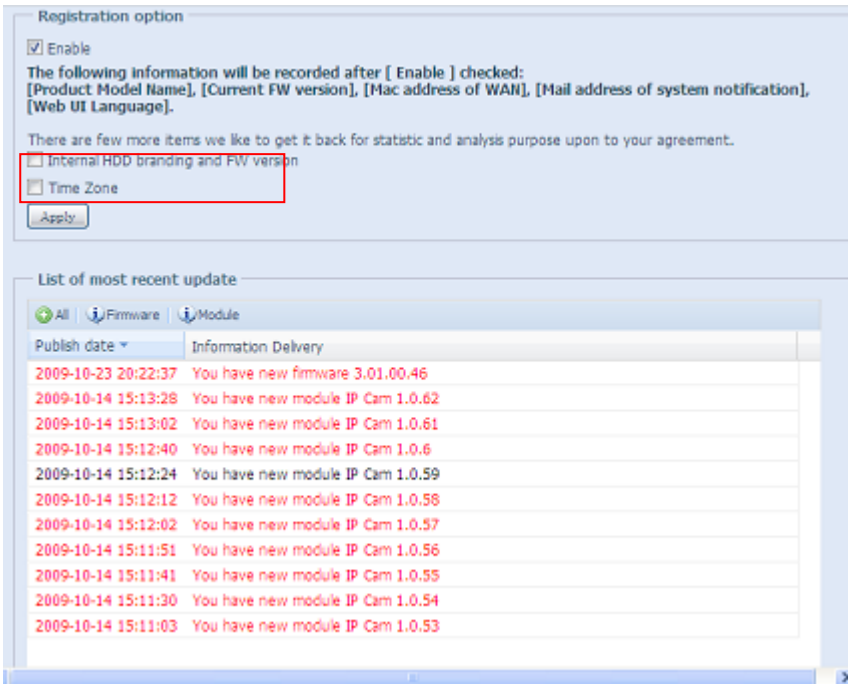
System Logs	
Item	**Description**
All	Provides all log information including system messages, warning messages and error messages.
INFO	Records information about system messages.
WARN	Shows only warning messages.
ERROR	Shows only error messages.
Download All Log File	Export all logs to an external file.
Truncate All Log File	Clear all log files.
The number of lines per page ☐	Specify desired number of lines to display per page.
Sort Ascending	Shows logs by date in ascending order.
Sort Descending	Shows logs by date in descending order.
|<< < > >>|	Use the forward (**>** **>>|**) and backward (**|<<** **<**) buttons to browse the log pages.
	Re-loading logs.

On-line Register

From the **System Information** menu, choose the **Online Registration** item and the **System Online Registration** screen appears. The online registration service can periodically update the user when new firmware and software modules are released by Thecus. To enable this service, simply check the "Enable" check box. By enabling this service, the items in bold will be sent to Thecus via the Internet.



Other than the defined items sent upon registration, there are also two additional items: "HDD Info" and "Time Zone". These two optional items can also be sent to Thecus anonymously for analysis and statistics purposes. To send these items, simply check the desired checkboxes to help Thecus improve its products and services.

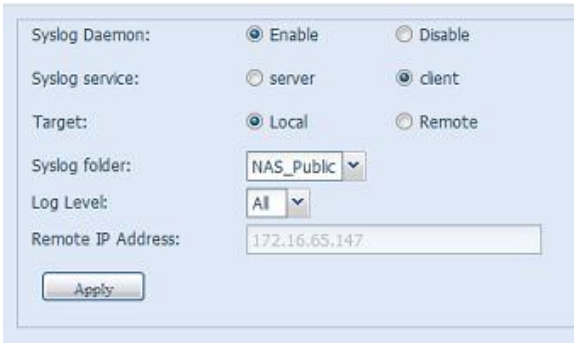

Registration option
Enable
The following information will be recorded after [Enable] checked:
[Product Model Name], [Current FW version], [Mac address of WAN], [Mail address of system notification], [Web UI Language].
There are few more items we like to get it back for statistic and analysis purpose upon to your agreement.
Internal HDD branding and FW version
Time Zone
Apply
List of most recent update
All
Firmware
Module
Publish date
Information Delivery
2009-10-23 20:22:37 You have new firmware 3.01.00.46
2009-10-14 15:13:28 You have new module IP Cam 1.0.62
2009-10-14 15:13:02 You have new module IP Cam 1.0.61
2009-10-14 15:12:40 You have new module IP Cam 1.0.6
2009-10-14 15:12:24 You have new module IP Cam 1.0.59
2009-10-14 15:12:12 You have new module IP Cam 1.0.58
2009-10-14 15:12:02 You have new module IP Cam 1.0.57
2009-10-14 15:11:51 You have new module IP Cam 1.0.56
2009-10-14 15:11:41 You have new module IP Cam 1.0.55
2009-10-14 15:11:30 You have new module IP Cam 1.0.54
2009-10-14 15:11:03 You have new module IP Cam 1.0.53

Syslog Management

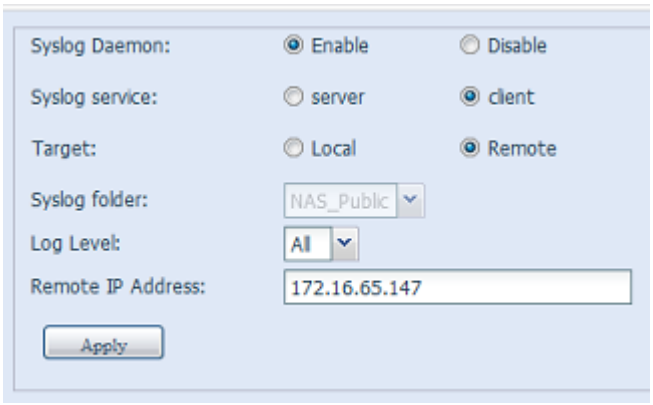
Generates system log to be stored locally or remotely, it also can be chose to act as syslog server for all other devices.
These messages are stored on your NAS in: Nsync > log> messages.
Information can be obtained in two ways: locally and remotely.

Configuration with syslog server:

Configuration with syslog client and target to store locally:



Configuration with syslog client and target to store remotely:



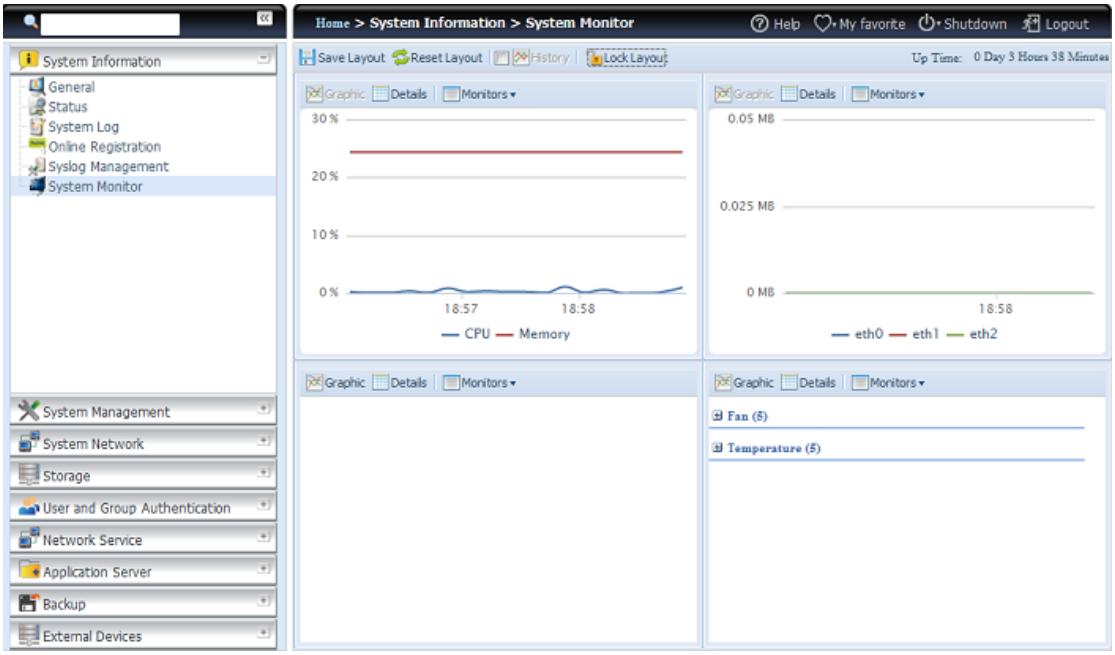
See the following table for a detailed description of each item:

Time	
Item	**Description**
Syslog Daemon	Enable/Disable syslog daemon.
Syslog service	If Server has been selected then associated syslog folder will be used to store all system logs from other NAS devices which has assigned this system for syslog server as well as syslog of this server unit. It can be seen from associated syslog folder with files "error", "Information" and "warning". If client has been selected then "Local" or "Remotely" can be choose.
Target	Choose Local, all system logs will be stored in an associated syslog folder filled in from next filed. And the syslog folder will have file "messages" to store all system logs. If Remotely has been selected, a syslog server is needed and an IP address is required.
Syslog folder	Select from a drop down share list, all of the system logs will be stored on it. This syslog folder is applied to "syslog server" or "syslog client" with "local" selected.
Log Level	The user can choose from 3 different levels. "All", "Warning/Error" or "Error".
Remote IP Address	Input the syslog server IP address if choose to store syslog info remotely.

System Monitor

The system monitor is capable to monitor system status including CPU/memory utilization, fan/temperature status, network throughput and on-line user list in various protocols.

To monitor system status, simply click on "System Monitor" from the tree menu and the screen will appear as below.

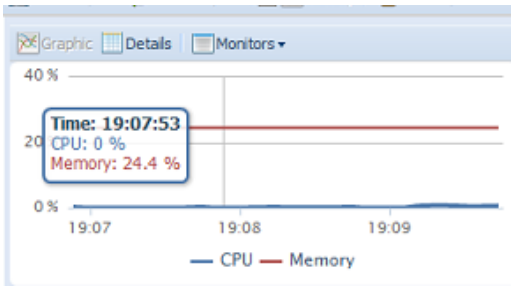


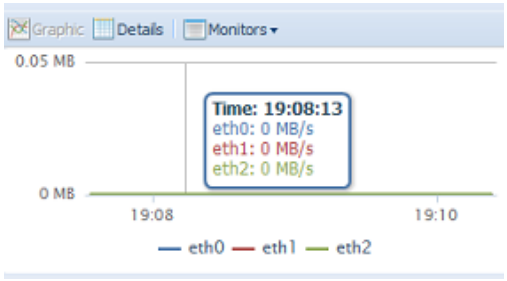
It is divided into 4 sections. Each section can be modified to monitor specific items by using the drop down list from the "Monitors" tab, simply click on the items you would like to monitor. From each section, you can also choose to display the information graphically by selecting "Graphic" or by plain text mode by selecting "Details".

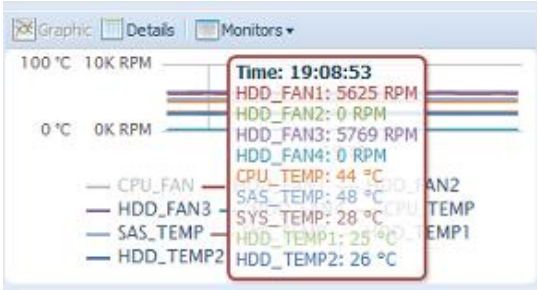
NOTE

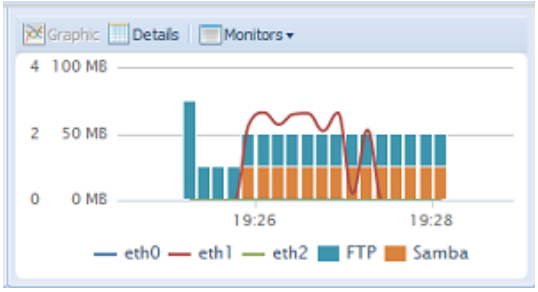
Only 2 sections can be set in graphic mode at the same time.

If graphic mode is chosen, 3 minutes of information is displayed on the x-axis. A resume of the information is displayed by dragging the mouse over the graphic at a specific time. See example below:

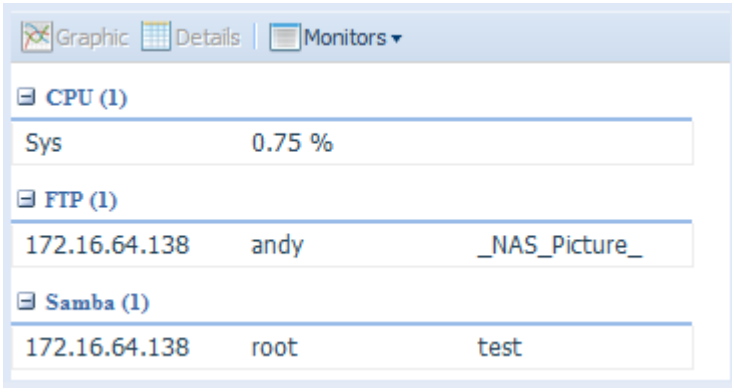




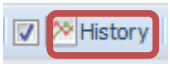




For the on-line users list, system monitor will display the on-line users and the share folder they have visited.



System Monitor	
Item	**Description**
Save Layout	Saving selected monitoring items. Layout will remain the same for future visits.
Reset Layout	Set back to default monitoring settings and layout.
History	Click on this check box and system monitor will write the monitoring history to a designate path in the RAID volume.
Lock Layout	All of the monitoring items are fixed and cannot be changed. Click again to unlock it.

If the History has been enabled, click on 

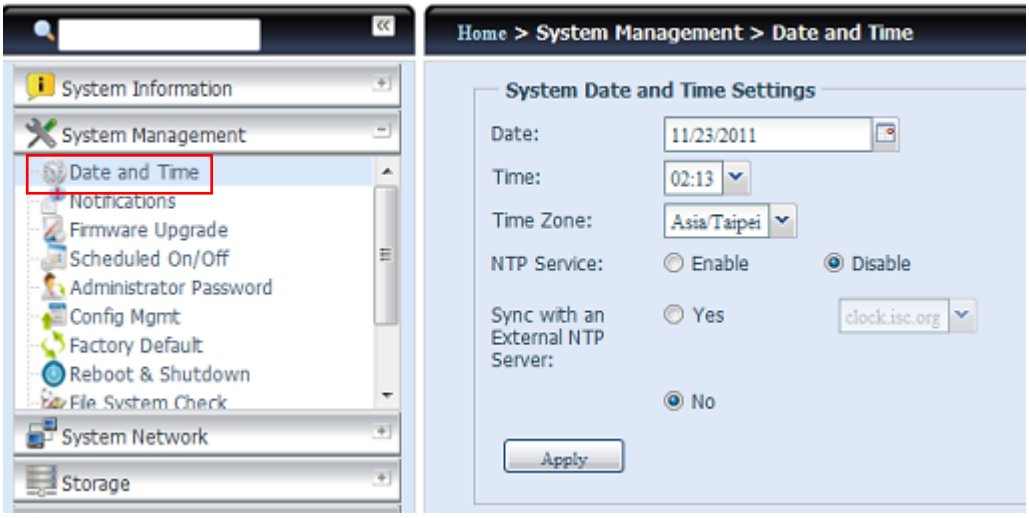
and system monitor will display the history with different period for selection.

System Management

The **System Management** menu gives you a wealth of settings that you can use to configure your Thecus IP storage system administration and functions. You can set up system time, system notifications, and even upgrade firmware from this menu.

Time: Setting system time

From the **time** menu, choose the **Time** item and the **Time** screen appears. Set the desired **Date**, **Time**, and **Time Zone**. You can also elect to synchronize the system time on Thecus IP storage with an **NTP (Network Time Protocol) Server**.



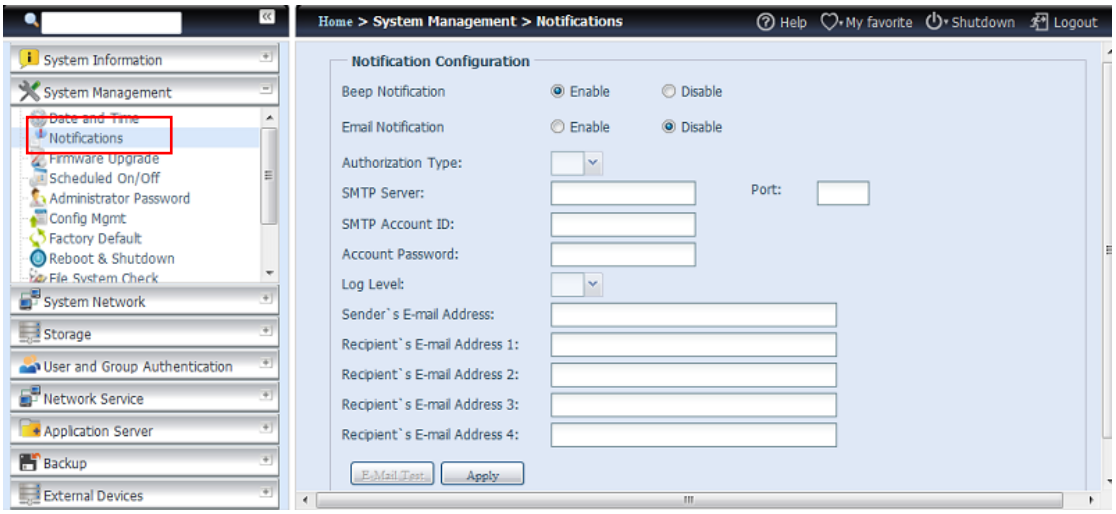
See the following table for a detailed description of each item:

Time	
Item	**Description**
Date	Sets the system date.
Time	Sets the system time.
Time Zone	Sets the system time zone.
NTP Service	Select ***Enable*** to synchronize with the NTP server. Select Disable to close the NTP server synchronization.
Sync with external NTP Server	Select **YES** to allow Thecus IP storage to synchronize with an NTP server of your choice. Press **Apply** to change.

WARNING If an NTP server is selected, please make sure your Thecus IP storage has been setup to access the NTP server.

Notification configuration

From the menu, choose the ***Notification*** item, and the **Notification Configuration** screen appears. This screen lets you have Thecus IP storage notify you in case of any system malfunction. Press ***Apply*** to confirm all settings. See following table for a detailed description of each item.



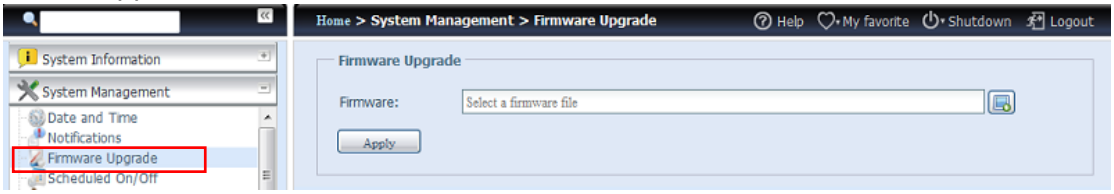
Notification Configuration	
Item	**Description**
Beep Notification	Enable or disable the system buzzer that beeps when a problem occurs.
Email Notification	Enable or disable email notifications of system problems.
Authentication Type	Select the SMTP Server account authentication type.
SMTP Server	Specifies the hostname/IP address of the SMTP server.
Port	Specifies the port to send outgoing notification emails.
SMTP Account ID	Set the SMTP Server Email account ID.
Account Password	Enter a new password.
Log Level	Select the log level to send the e-mail out.
Sender's E-mail Address	Set senders email address to send email notifications.
Receiver's E-mail Address (1,2,3,4)	Add one or more recipient's email addresses to receive email notifications.

NOTE

Consult with your mail server administrator for email server information.

Firmware Upgrade

From the menu, choose the ***Firmware Upgrade*** item and the **Firmware Upgrade** screen appears.



Follow the steps below to upgrade your firmware:

1. Use the ***Browse*** button to find the firmware file.
2. Press ***Apply***.
3. The buzzer will beep and the Busy LED will blink until the upgrade is complete.

NOTE

- The buzzer only beeps if it is enabled in the System Notification menu.
- Check Thecus website for the latest firmware release and release notes.
- Downgrading firmware is not permitted.

WARNING

Do not turns off the system during the firmware upgrade process.
This will lead to a catastrophic result that may render the system inoperable.

Schedule Power On/Off

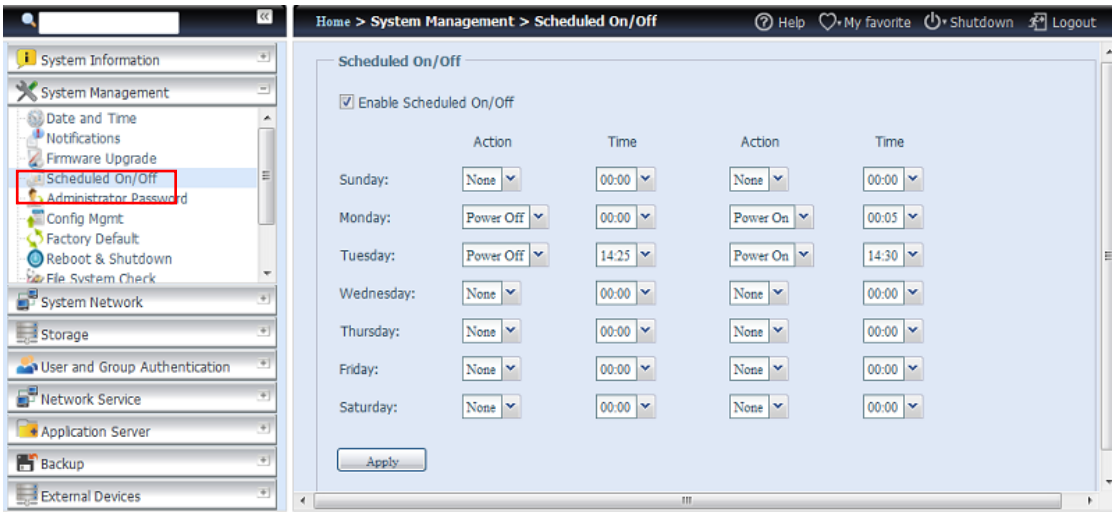
Using the Thecus IP storage System Management, you can save energy and money by scheduling the Thecus IP storage to turn itself on and off during certain times of the day.

From the menu, choose the **Schedule Power On/Off** item and the **Schedule Power On/Off** screen appears.

To designate a schedule for the Thecus IP storage to turn on and off, first enable the feature by checking the **Enable Schedule Power On/Off** checkbox.

Then, simply choose an on and off time for each day of the week.

Finally, click ***Apply*** to save your changes.



Example - Monday: On: 8:00; Off: 16:00
System will turn on at 8:00 AM on Monday, and off at 16:00 on Monday. System will turn on for the rest of the week.

If you choose an on time, but do not assign an off time, the system will turn on and remain on until a scheduled off time is reached, or if the unit is shutdown manually.

Example - Monday: On: 8:00
System will turn on at 8:00 AM on Monday, and will not shut down unless powered down manually.

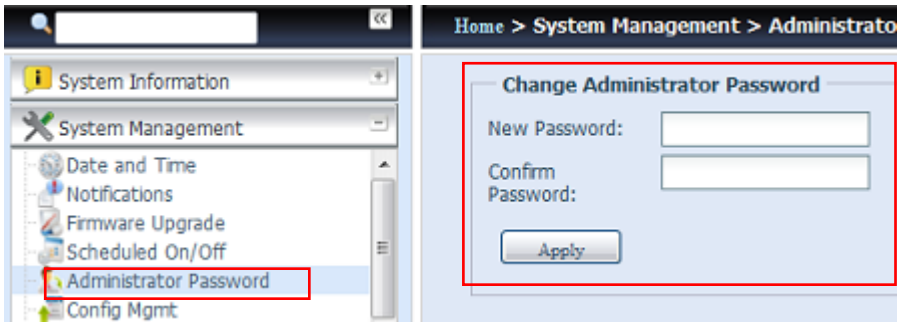
You may also choose two on times or two off times on a particular day, and the system will act accordingly.

Example - Monday: Off: 8:00; Off: 16:00
System will turn off at 8:00 AM on Monday. System will turn off at 16:00 PM on Monday, if it was on. If the system was already off at 16:00 PM on Monday, system will stay off.

Administrator Password

From the menu, choose the **Administrator Password** item and the **Change Administrator Password** screen appears. Enter a new password in the **New Password** box and confirm your new password in the **Confirm Password** box. Press ***Apply*** to confirm password changes.

There is also a **password** to enter the **OLED** setting that you can setup here. Enter a new password in the **New Password** box and confirm your new password in the **Confirm Password** box. Press ***Apply*** to confirm password changes.

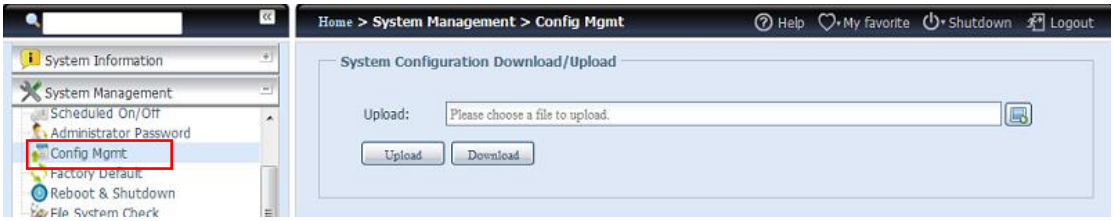


See the following table for a detailed description of each item.

Change Administrator and LCD Entry Password	
Item	**Description**
New Password	Type in a new administrator password.
Confirm Password	Type the new password again to confirm.
Apply	Press this to save your changes.

Config Mgmt

From the menu, choose the ***Config Mgmt*** item and the **System Configuration Download/Upload** screen appears. From here, you can download or upload stored system configurations.



See the following table for a detailed description of each item.

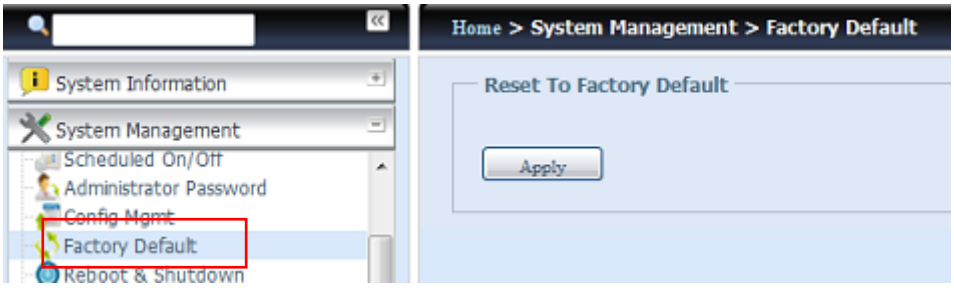
System Configuration Download/Upload	
Item	**Description**
Download	Save and export the current system configuration.
Upload	Import a saved configuration file to overwrite the current system configuration.

NOTE

Backing up your system configuration is a great way to ensure that you can revert to a working configuration when you are experimenting with new system settings. The system configuration you have backed up can only be restored in the same firmware version. The backup details exclude user/group accounts.

Factory Default

From the menu, choose the ***Factory Default*** item and the **Reset to Factory Default** screen appears. Press ***Apply*** to reset Thecus IP storage to factory default settings.



WARNING Resetting to factory defaults will not erase the data stored in the hard disks, but WILL revert all the settings to the factory default values.

Reboot & Shutdown

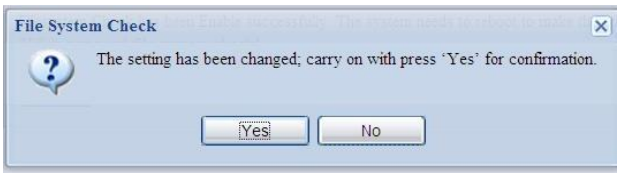
From the menu, choose **Reboot & Shutdown** item, and the **Shutdown/Reboot System** screen appears. Press ***Reboot*** to restart the system or ***Shutdown*** to turn the system off.

File System Check

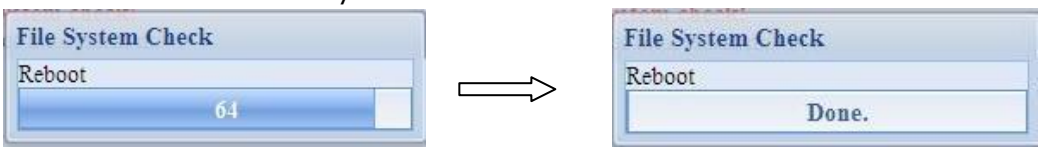
The File System Check allows you to perform a check on the integrity of your disks' file system. Under the menu, click ***File system Check*** and the **File System Check** prompt appears.

Home > System Management > File System Check
Help
My favorite
System Information
System Management
Scheduled On/Off
Administrator Password
Config Mgmt
Factory Default
Reboot & Shutdown
File System Check
File System Check
The file system has been checked successfully. Reboot the system make the changes effective.
Encrypted RAID does not support file system checks!
Press [Apply] to reboot the system now.
Apply

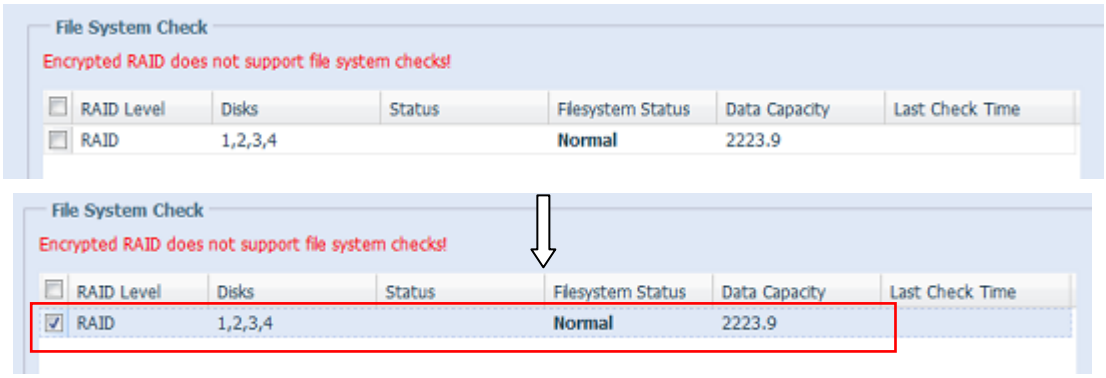
To perform a file system check, click ***Apply***.
Once clicked, the following prompt will appear:



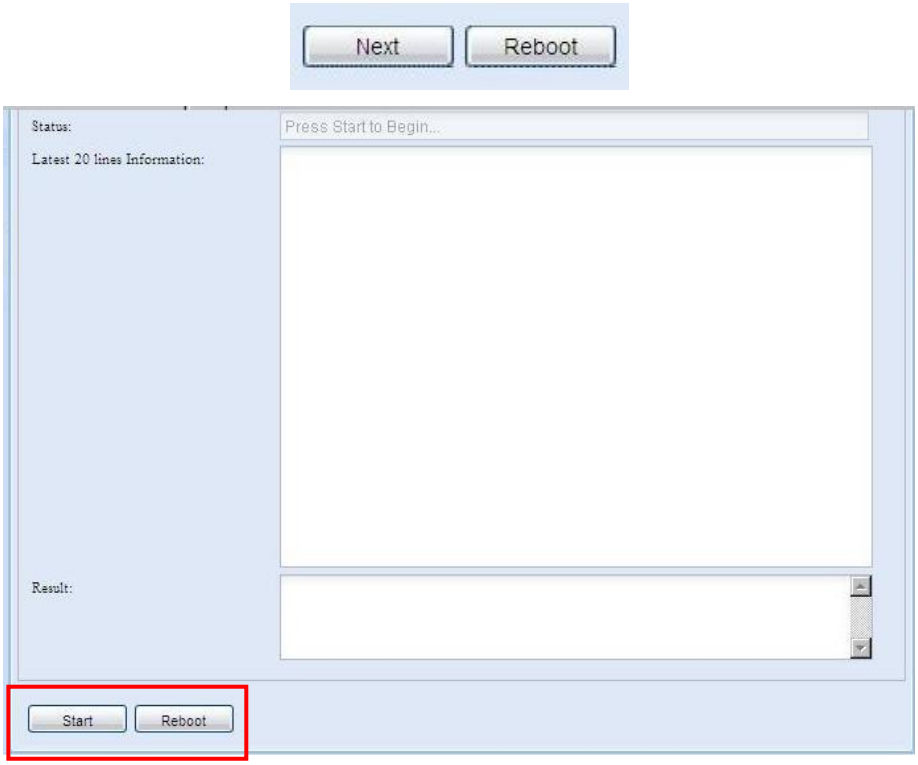
Click ***Yes*** to reboot the system.



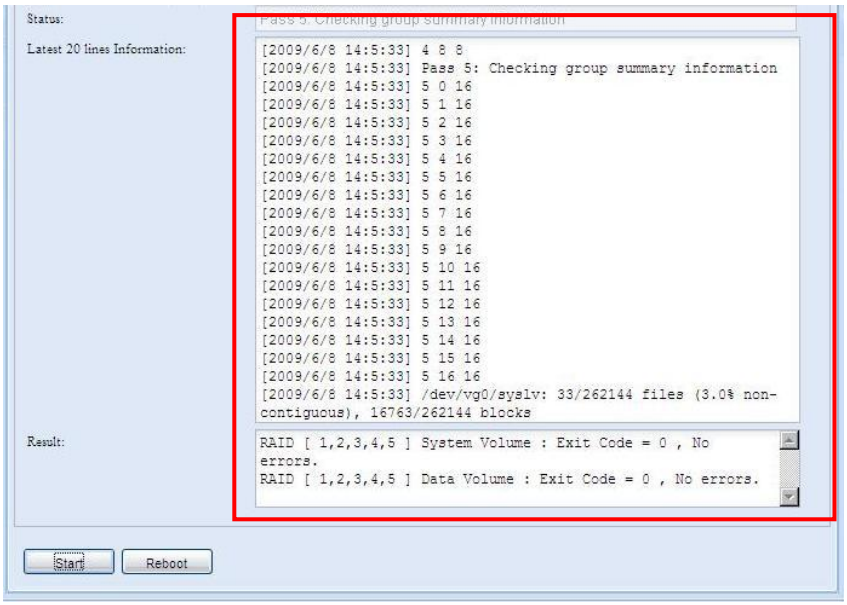
Once the system has rebooted, you will be returned to the **File System Check** prompt. There you will see the available RAID volumes to run the file system check. Check the desired RAID volumes and click ***Next*** to proceed with the file system check. Click ***Reboot*** to reboot without running the check.



Once you click ***Next***, you will see the following screen:



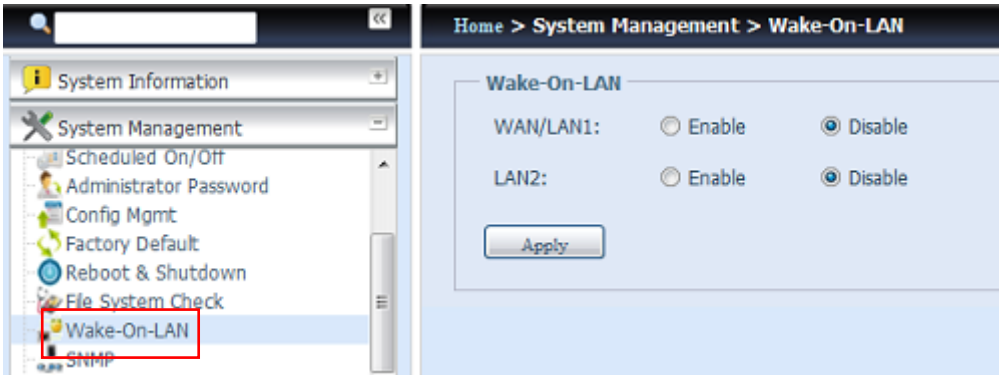
Click ***Start*** to begin the file system check. Click ***Reboot*** to reboot the system. When the file system check is running, the system will show 20 lines of information until it is complete. Once complete, the results will be shown at the bottom.



NOTE The system must be rebooted before Thecus IP storage can function normally after file system check completes.

Wake-Up On LAN (WOL)

The Thecus IP storage has the ability to be awoken from sleep mode via WAN/LAN1 or LAN2 port.



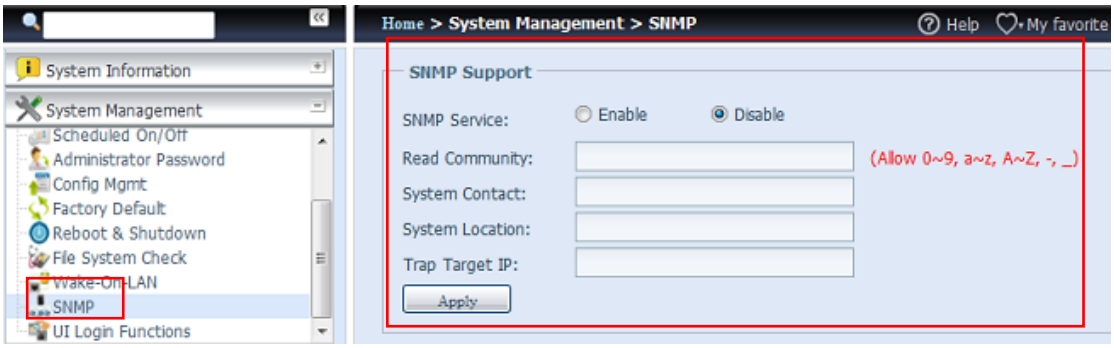
From the menu, choose the ***WOL*** item, and the **Wake-up On LAN** screen appears. From here, you can **Enable** or **Disable**.

Wake-up On LAN Configuration	
Item	**Description**
WAN/LAN1	**Enable** or **Disable** WOL service from WAN/LAN1
LAN2	**Enable** or **Disable** WOL service from LAN2
Apply	Click ***Apply*** to save changes.

SNMP Support

From the menu, choose the **SNMP** item and the **SNMP Support** screen appears. You could enable the SNMP function and filled in the related information in each

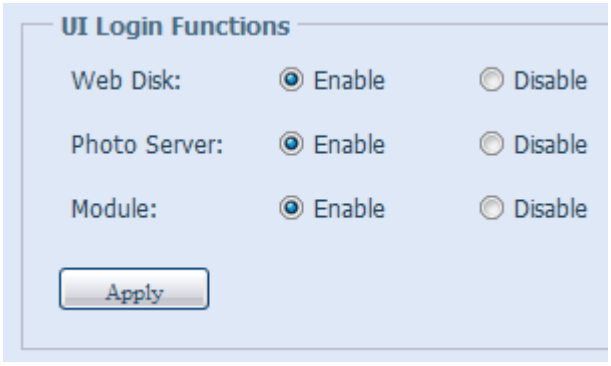
fields. With the SNMP management software, you can get other system's basic information.



From the menu, choose the **SNMP** item, and the **SNMP Support** screen appears. From here, you can **Enable** or **Disable**.

UI Login Function

Adjusts UI Login Configuration settings, you can enable/disable the Web Disk, Photo Server and modules functions, according to your needs.

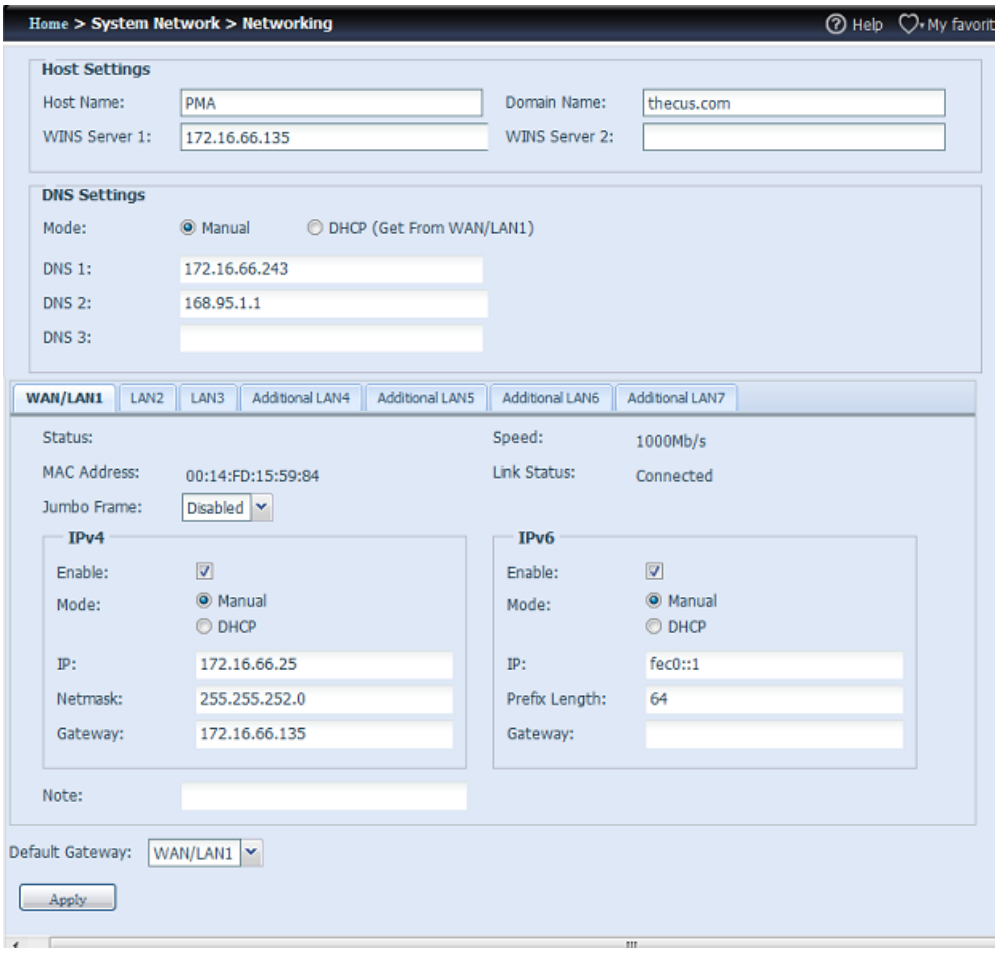


System Network

Use the **System Network** menu to make network configuration settings to an on board network port or additional NIC as well as DHCP and link aggregation.

Networking

From the **System Network** menu, choose ***Networking***, and the **Networking Configuration** screen appears. This screen displays the network parameters of the global setting and available network connection. You may change any of these items and press ***Apply*** to confirm your settings. See a description of each item in the following table:



The available system network ports are coming from embedded system ports and additional system ports added through the reserved PCI-e slot with associated compatible list. Therefore, the screen shown above is an example of a Thecus N16000 with 3 on board GbE NIC and an additionally Intel PRO/1000 PT quad port NIC, for a total of 7 NIC ports.

Network Configuration (Global parameter)	
Item	**Description**
Host name	Host name that identifies the Thecus IP storage on the network.
Domain name	Specifies the domain name of Thecus IP storage.
WINS Server	To set a server name for NetBIOS computer.
DNS Mode	Select the DNS server is coming from DHCP server or manual input. A total of 3 DNS servers can be input. If the DNS setting is chosen from DHCP server, then it will refer to WAN/LAN1 port.
DNS Server 1,2,3	Domain Name Service (DNS) server IP address.

Network Configuration (NIC port)	
Link speed	Display associated NIC port link speed.
Link status	Display associated NIC port link status.
MAC address	MAC address of the network interface.
Jumbo Frame Support	Enable or disable Jumbo Frame Support of associate interface on your Thecus IP storage.
IPv4/IPv6	Click to enable IPv4/IPv6 for TCP/IP. The default is IPv4 enabled.
Mode	It can choose a static IP or Dynamic IP.
IP	IP address of associate NIC interface.
Netmask/Prefix Length	Input netmask for IPv4 and Prefix length for IPv6.
Gateway	Gateway for associate NIC.
Default gateway	It can be chosen from a drop down list of default gateway that's been used for the Thecus IP storage.

NOTE

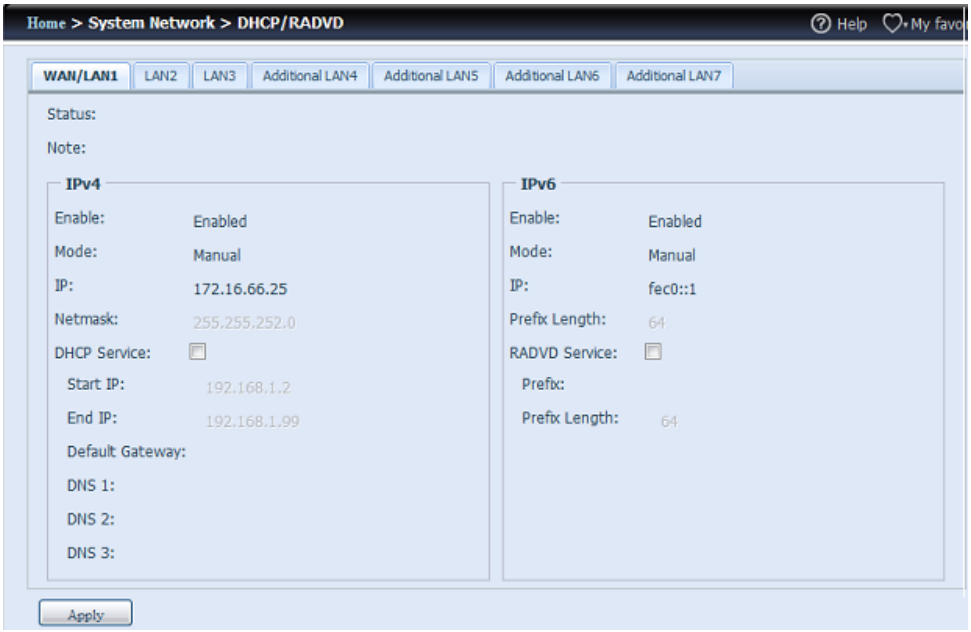
- Only use Jumbo Frame settings when operating in a Gigabit environment where all other clients have Jumbo Frame Setting enabled.
- Proper DNS setting is vital to networks services, such as SMTP and NTP.

WARNING

Most faster Ethernet (10/100) Switches/Routers do not support Jumbo Frame and will not be able to connect to your Thecus NAS after Jumbo Frame is turned on.

DHCP/RADVD

From the **System Network** menu, choose ***DHCP/RADVD***, and the **DHCP/RADVD Configuration** screen appears. This screen displays available NIC status. If each NIC has been set-up to a static IP, then each NIC can be configured to act as DHCP/RADVD server.



DHCP/RADVD Server Configuration

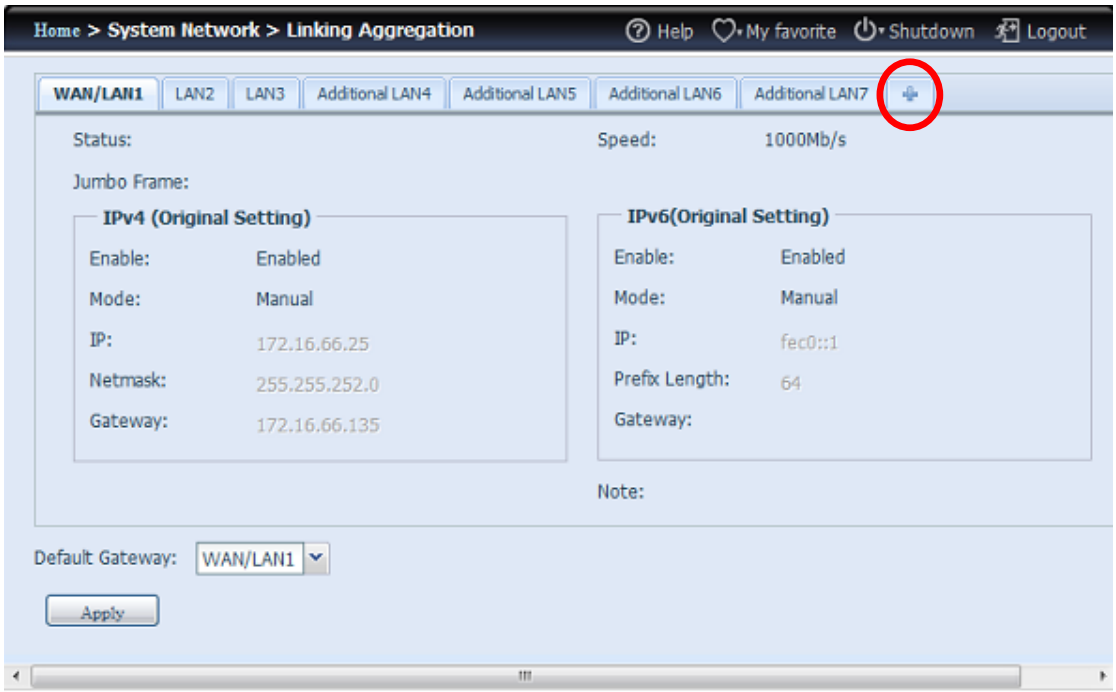
A DHCP/RADVD server can be configured to assign IP addresses (IPv4) or Prefix (IPv6) to devices connected to the associated NIC port.

DHCP Configuration	
Item	**Description**
DHCP/RADVD Service	Enable or disable the DHCP/RADVD service to automatically assign IP address to PCs connected to associate NIC interface.
Start IP (IPv4)	Specifies the lower IP address of the DHCP range.
End IP in (IPv4)	Specifies the highest IP address of the DHCP range.
Default Gateway (IPv4)	Specifies gateway for the DHCP server service.
DNS Server 1,2,3 (IPv4)	Displayed the DNS server IP address.
Prefix (IPv6)	Specifies prefix
Prefix Length (IPv6)	Specifies prefix length

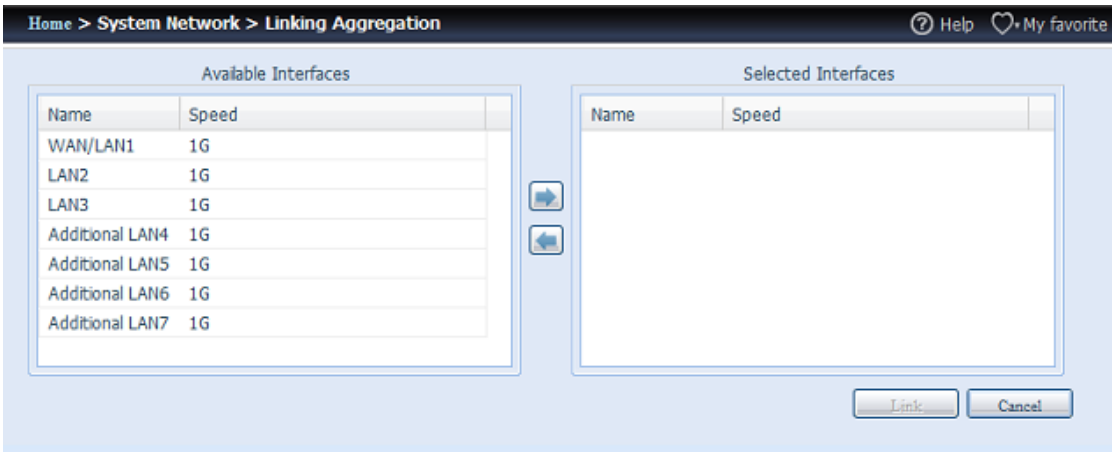
WARNING The IP address of associated NIC should not be in the range of the Start IP address and End IP address (IPv4).

Linking Aggregation

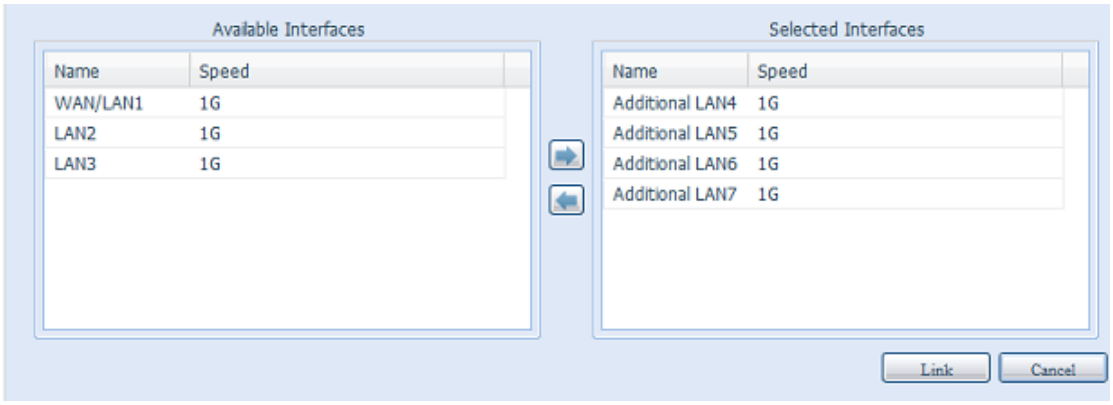
The Thecus IP storage supports link aggregation from either on board network port or additional NIC. Simply click on "+" as shown in the screen shot below.



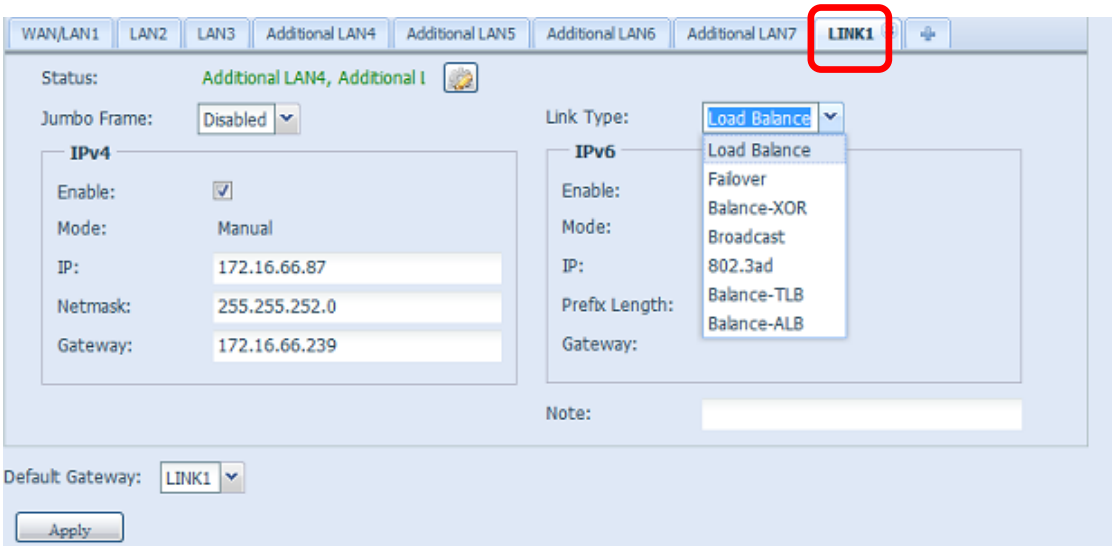
The associated screen shot will appear after the "+" is clicked.



Select from available network port then move over to selected box.



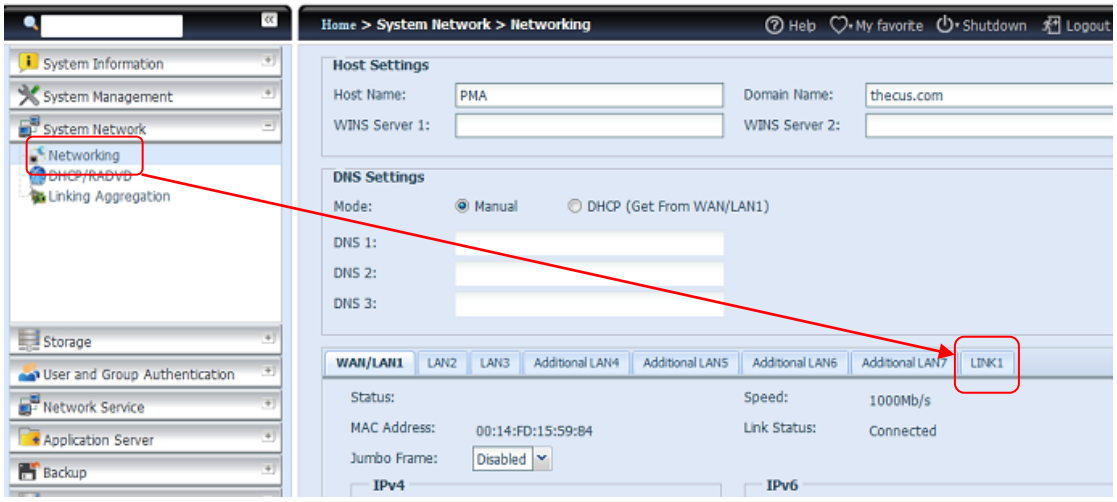
Click "Link" to confirm the selection. The newly created tab will appear for more settings required to complete the link aggregation configuration.



Link1 Configuration	
Status	Specifies the network ports being used with the associated link aggregation. Click on to modify the selected network ports.

Jumbo Frame Support	Enable or disable Jumbo Frame Support of the associated interface on your Thecus IP storage.
Link Type	Select from drop down list for desired mode.
IPv4/IPv6	Click to enable IPv4/IPv6 for TCP/IP. The default is IPv4 enabled.
Mode	It has to be a static IP with the link aggregation being used.
IP	IP address of link aggregation.
Netmask/Prefix Length	Input netmask for IPv4 and Prefix length for IPv6.
Gateway	Gateway for associated link aggregation
Default gateway	It can be chosen from the drop down list of default gateway being used for the Thecus IP storage.

Now under the networking, a "Link1" tab will appear from the network title bar.



To modify or delete LINK1, go to Link Aggregation setting page. Click on

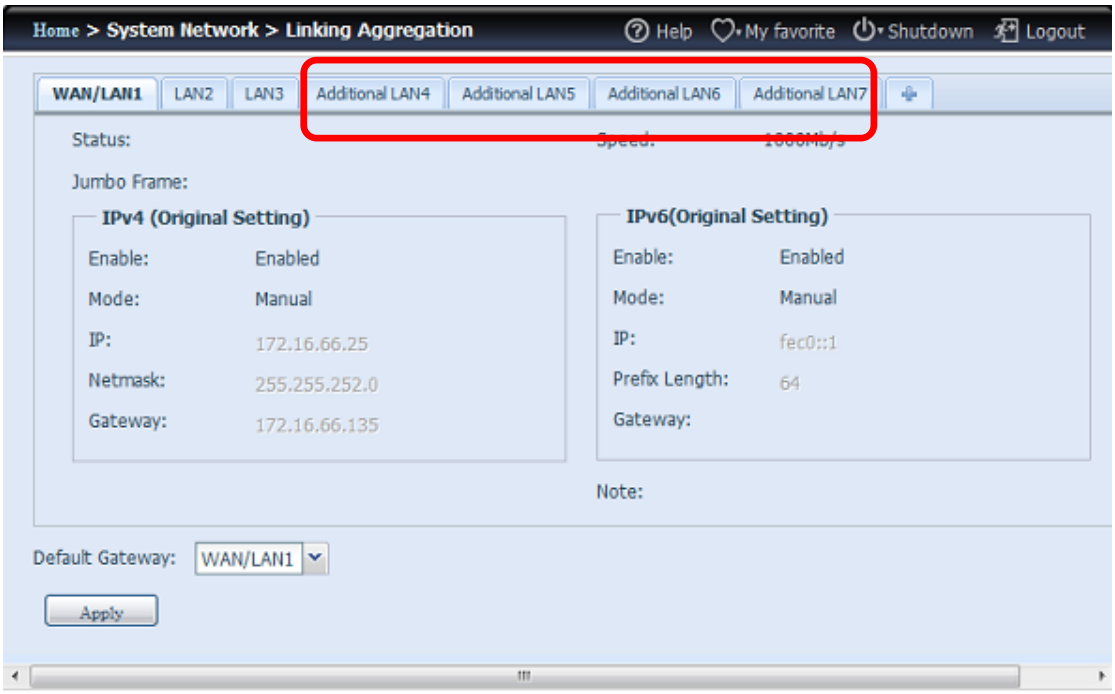
to modify the settings or click on

to delete this link aggregation. If any ports are still available, additional link aggregation links can be created by clicking .

Additional LAN

Other than on-board LAN port, Thecus IP storage supports additional NIC to be added in its available PCI-e slot. For the details of additional NIC support list please visit Thecus website.
http://www.thecus.com/sp_comlist.php

Once the additional NIC is installed into Thecus IP storage, the "Additional LANx" will appear under the "Networking" category. Click the associated NIC to setup the details. The screen shot below shows an example of an Intel PRO/1000 PT Quad port installed thru a PCI-e slot in the Thecus IP storage.



Storage Management

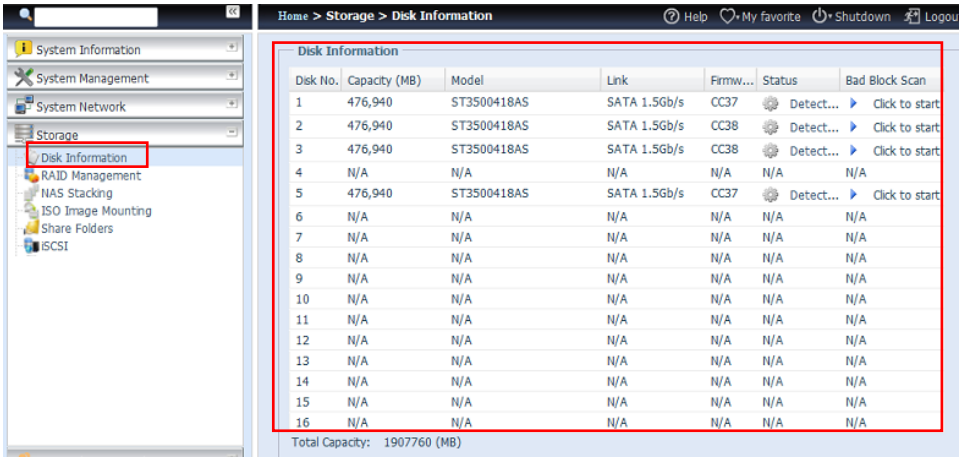
The **Storage** menu displays the status of storage devices installed in the Thecus IP storage. It includes storage configuration options such as RAID and disk settings, folder configuration, iSCSI and ISO Mount.

Disks Information (Refer Chapter 7 for FW v2.03.01 and after)

From the **Storage** menu, choose the ***Disk Information*** item and the **Disk Information** screen appears. From here, you can see various installed SATA/SAS hard disks. A blank line indicates that a hard disk is not currently installed in that particular disk slot.

NOTE

- The screen shot below is just an example from a Thecus IP Storage. The disk slots number can range from 8, 12 to 16 slots depending on the model of Thecus IP storage.


Home > Storage > Disk Information
Help
My favorite
Shutdown
System Information
System Management
System Network
Storage
Disk Information
RAID Management
NAS Stacking
ISO Image Mounting
Share Folders
iSCSI
Disk Information
Disk No. | Capacity (MB) | Model | Link | Firmw... | Status | Bad Block Scan
1 476,940 ST3500418AS SATA 1.5Gb/s CC37 Detect... Click to start
2 476,940 ST3500418AS SATA 1.5Gb/s CC38 Detect... Click to start
3 476,940 ST3500418AS SATA 1.5Gb/s CC38 Detect... Click to start
4 N/A N/A N/A N/A N/A N/A
5 476,940 ST3500418AS SATA 1.5Gb/s CC37 Detect... Click to start
6 N/A N/A N/A N/A N/A N/A
7 N/A N/A N/A N/A N/A N/A
8 N/A N/A N/A N/A N/A N/A
9 N/A N/A N/A N/A N/A N/A
10 N/A N/A N/A N/A N/A N/A
11 N/A N/A N/A N/A N/A N/A
12 N/A N/A N/A N/A N/A N/A
13 N/A N/A N/A N/A N/A N/A
14 N/A N/A N/A N/A N/A N/A
15 N/A N/A N/A N/A N/A N/A
16 N/A N/A N/A N/A N/A N/A
Total Capacity: 1907760 (MB)

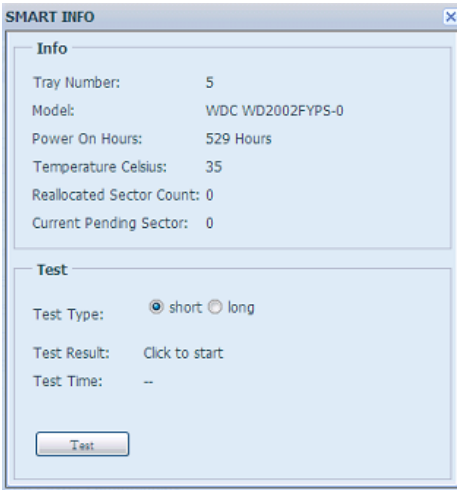
Disks Information	
Item	**Description**

Disk No.	Indicates disk location.
Capacity	Shows the SATA hard disk capacity.
Model	Displays the SATA hard disk model name.
Link	Displays the hard disk interface and link speed
Firmware	Shows the SATA hard disk firmware version.
Status	Indicates the status of the disk.
Bad Block scan	Yes to start scan Bad Block.

S.M.A.R.T. Information

On the **Disk Information** screen, the status of each disk will be displayed in the **Status** column. Clicking on the ***OK*** or ***Warning*** link will display the **S.M.A.R.T Information** window for that particular disk.

You may also perform disk SMART test (doesn't apply to SAS HDD); simply click "Test" to start the SMART test. The result is only for reference and the system will not take any action from its result.



S.M.A.R.T. Information	
Item	**Description**
Tray Number	Tray the hard disk is installed in.
Model	Model name of the installed hard disk.
Power ON Hours	Count of hours in power-on state. The raw value of this attribute shows total count of hours (or minutes, or seconds, depending on manufacturer) in power-on state.
Temperature Celsius	The current temperature of the hard disk in degrees Celsius.
Reallocated Sector Count	Count of reallocated sectors. When the hard drive finds a read/write/verification error, it marks this sector as "reallocated" and transfers data to a special reserved area (spare area). This process is also known as remapping and "reallocated" sectors are called remaps. This is why, on a modern hard disks, you cannot see "bad blocks" while testing the surface - all bad blocks are hidden in reallocated sectors. However, the more sectors that are reallocated, the more a decrease (up to 10% or more) can be noticed in disk read/write speeds.
Current Pending Sector	Current count of unstable sectors (waiting for remapping). The raw value of this attribute indicates the total number of sectors waiting for remapping. Later, when some of these sectors are read successfully, the value is decreased. If errors still occur when reading sectors, the hard drive will try to restore the data,

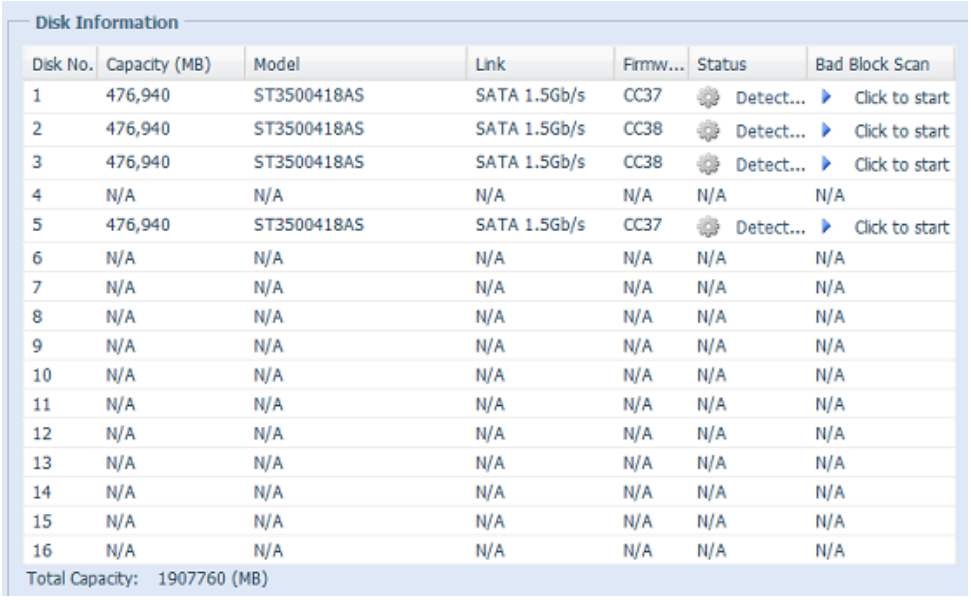
	transfer it to the reserved disk area (spare area), and mark this sector as remapped. If this attribute value remains at zero, it indicates that the quality of the corresponding surface area is low.
Test Type	Set short or long time to test.
Test Result	Result of the test.
Test Time	Total time of the test.

NOTE

If the Reallocated Sector Count > 32 or Current Pending Sector of a hard disk drive > 0 , the status of the disk will show "Warning". This warning is only used to alert the system administrator that there are bad sectors on the disk, and they should replace those disks as soon as possible.

Bad Block Scan

On the **Disk Information** screen, you may also perform disk bad block scan, simply click "Click to start" to start the scan. The result is only for reference and the system will not take any action from its result.

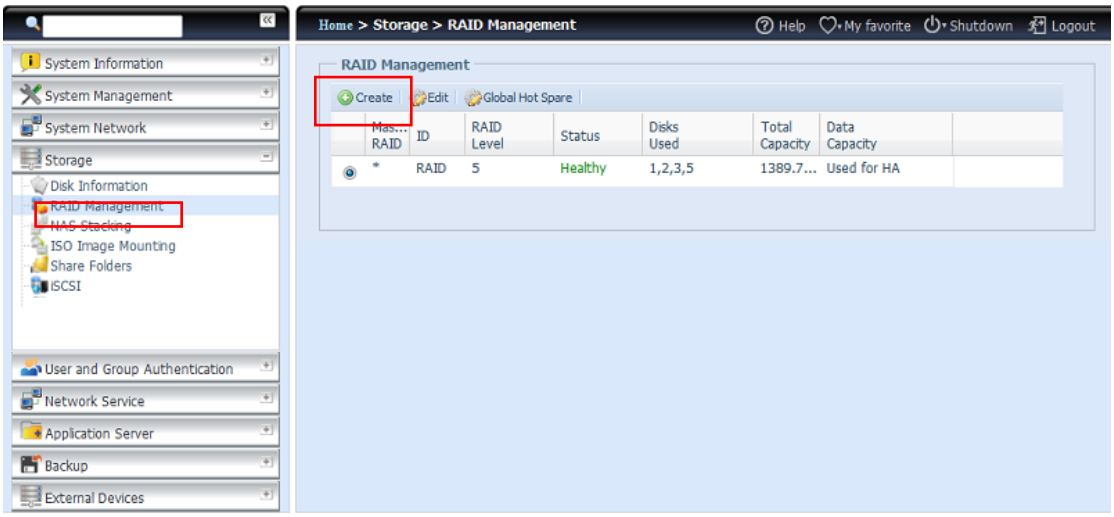

Disk Information
Disk No. Capacity (MB) Model Link Firmw... Status Bad Block Scan
1 476,940 ST3500418AS SATA 1.5Gb/s CC37 Detect... Click to start
2 476,940 ST3500418AS SATA 1.5Gb/s CC38 Detect... Click to start
3 476,940 ST3500418AS SATA 1.5Gb/s CC38 Detect... Click to start
4 N/A N/A N/A N/A N/A N/A
5 476,940 ST3500418AS SATA 1.5Gb/s CC37 Detect... Click to start
6 N/A N/A N/A N/A N/A N/A
7 N/A N/A N/A N/A N/A N/A
8 N/A N/A N/A N/A N/A N/A
9 N/A N/A N/A N/A N/A N/A
10 N/A N/A N/A N/A N/A N/A
11 N/A N/A N/A N/A N/A N/A
12 N/A N/A N/A N/A N/A N/A
13 N/A N/A N/A N/A N/A N/A
14 N/A N/A N/A N/A N/A N/A
15 N/A N/A N/A N/A N/A N/A
16 N/A N/A N/A N/A N/A N/A
Total Capacity: 1907760 (MB)

The testing result will display "Click to start" as default until the system reboots.

RAID Information

From the **Storage** menu, choose the ***RAID Management*** item and the **RAID Management** screen appears.

This screen lists the RAID volumes currently residing in the Thecus IP storage. From this screen, you can get information about the status of your RAID volumes, as well as the capacities allocated for data.



RAID Information	
Item	**Description**
Master RAID	The RAID volume currently designated as the Master RAID volume.
ID	ID of the current RAID volume. **NOTE: All RAID IDs must be unique.**
RAID Level	Shows the current RAID configuration.
Status	Indicates status of the RAID. Can read either ***Healthy***, ***Degraded***, or ***Damaged***.
Disks Used	Hard disks used to form the current RAID volume.
Total Capacity	Total capacity of the current RAID.
Data Capacity	Indicates the used capacity and total capacity used by user data.

Create a RAID

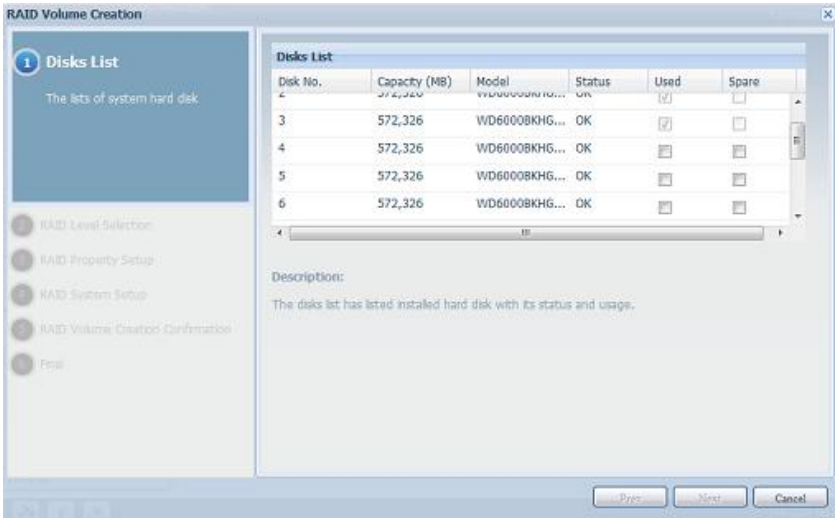
On the **RAID Information** screen, press the ***Create*** button to go to the **RAID Volume Creation** screen. In addition to RAID disk information and status, this screen lets you make RAID configuration settings.
Using **Create RAID**, you can select stripe size, choose which disks are RAID disks or the Spare Disk. .

RAID Configurations	
Item	**Description**
Disk No.	Number assigned to the installed hard disks.
Capacity (MB)	Capacity of the installed hard disks.
Model	Model number of the installed hard disks.
Status	Status of the installed hard disks.
Used	If this is checked, current hard disk is aalready part of a RAID volume.
Spare	If this is checked, current hard disk is designated as a spare for a RAID volume.
Master RAID	Check a box to designate this as the Master RAID volume. See the **NOTE** below for more information.
Stripe Size	This sets the stripe size to maximize performance of sequential files in a storage volume. Keep the 64K setting unless you require a special file storage layout in the storage volume. A larger stripe size is better for large files.
Data Percentage	The percentage of the RAID volume that will be used to store data.
Create	Press this button to configure a file system and create the RAID

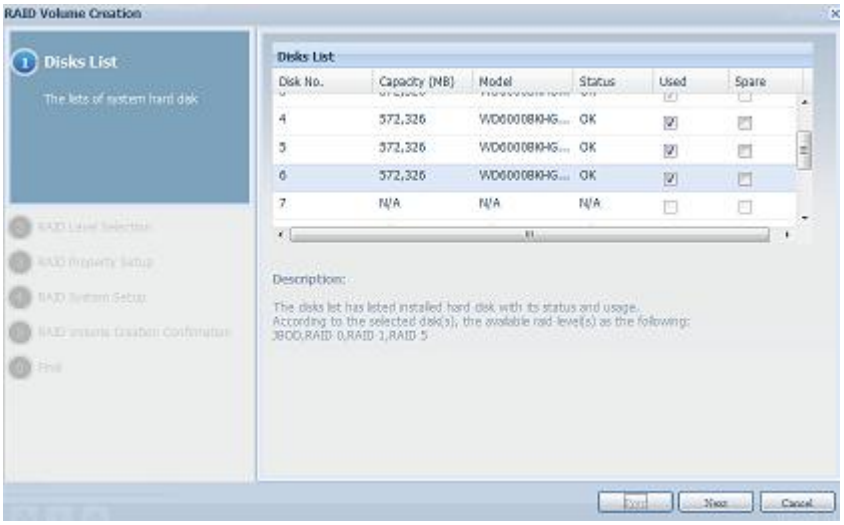
	storage volume.

To create a RAID volume, follow the steps below:

1. On the **RAID Information** screen, clicks create.



2. On the **RAID Configuration** screen, set the RAID storage space as **JBOD**, **RAID 0**, **RAID 1**, **RAID 5**, **RAID 6, RAID 10, RAID 50** or **RAID 60** (depends on model)— see **Appendix B: RAID Basics** for a detailed description of each.



NOTE N8900/N12000/N16000 Series supports multiple RAID modes and are capable of creating up to five RAID volumes within a single NAS system.

3. Specify a RAID ID.

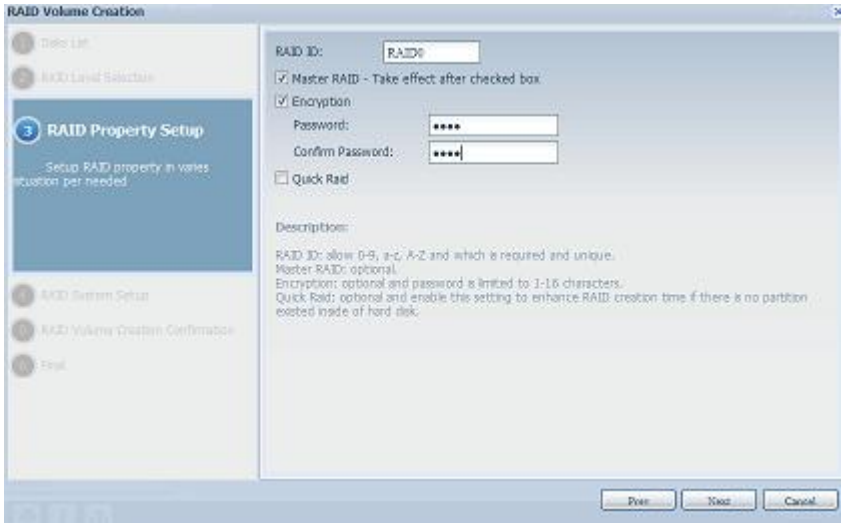
RAID Volume Creation
RAID Level Selection
System will list available RAID level can be choose from
RAID Level
JBOD
RAID 0
RAID 1
RAID 5
Description:
JBOD: Combine multiple drives and capacities into one drive.
RAID 0: Normally used to increase performance and useful for setups such as large read-only NFS server where mounting many disks is time-consuming or impossible and redundancy is irrelevant.
RAID 1: Create an exact copy (or mirror) of a set of data on two or more disks. This is useful when

4. If this RAID volume is meant to be the Master RAID volume, tick the **Master RAID** checkbox.

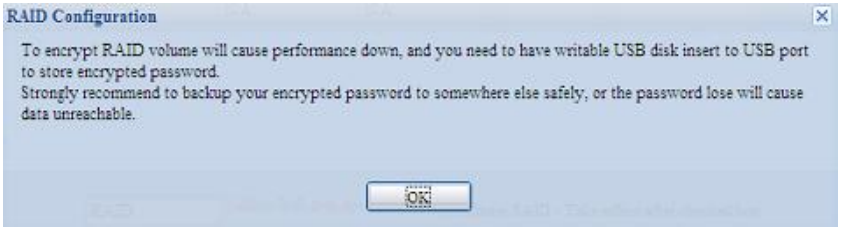
NOTE

In a multiple RAID configuration, one RAID volume must be designated as the Master RAID volume. The Master RAID volume will store all installed modules. If the Master RAID is changed to another location (i.e. assigning volume 2 to be the Master RAID volume after volume 1 had been previously assigned), then all modules must be reinstalled. In addition, all system folders that were contained on the Master RAID volume will be invisible. Reassigning this volume to be the Master RAID will make these folders visible again.

5. Selected whether the RAID volume will be encrypted or not.
   The RAID volume can protect data by using RAID Volume Encryption function to prevent the risk of data exposure. To activate this function, the **Encryption** option needs to be enabled while the RAID is created and followed by a password input for identification. Also, an external writable USB disk plugged into any USB port on the system is required to save the password you have entered while the RAID volume is being created. See the screenshot below for details.



Once the **Create** button has been pressed with the **Encryption** checkbox enabled, the following message pop-up will appear for confirmation.


RAID Configuration
To encrypt RAID volume will cause performance down, and you need to have writable USB disk insert to USB port to store encrypted password.
Strongly recommend to backup your encrypted password to somewhere else safely, or the password lose will cause data unreachable.
OK

After the RAID volume has been created, you may remove the USB disk until the next time the system boots. The RAID volume cannot be mounted if the USB disk with the encryption key isn't found in any system USB port when the volume is accessed. To activate the encrypted volume, plug the USB disk containing the encryption key and into any system USB port.

We strongly recommended copying the RAID volume encryption key to a safe place. You can find the encryption key file from the USB disk in the following format:

(RAID volume created date)_xxxxxx.key

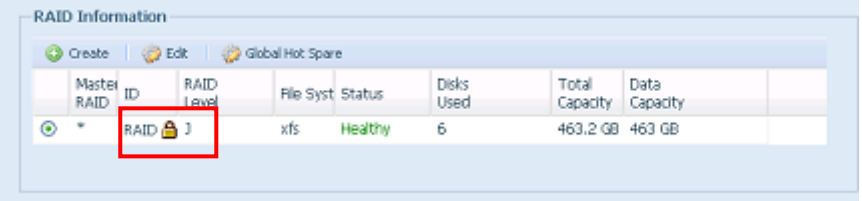
WARNING

Please keep your USB disk in a safe place and also backup the encrypted key.
There is no way to rescue data back if the key is lost.

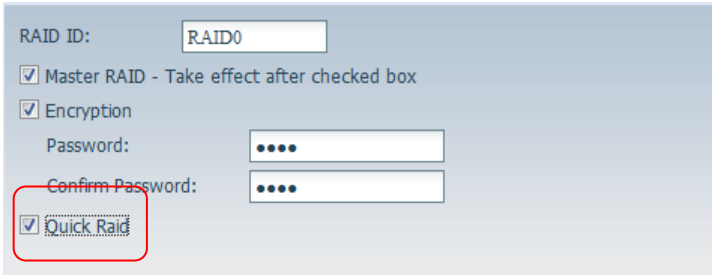
NOTE

With RAID volume encryption enabled, the system performance will go down.

RAID volumes with encryption enabled will be displayed with a key lock symbol next to volume ID name.



6. Quick RAID — Enabled the quick RAID setting is going to enhance RAID creation time.

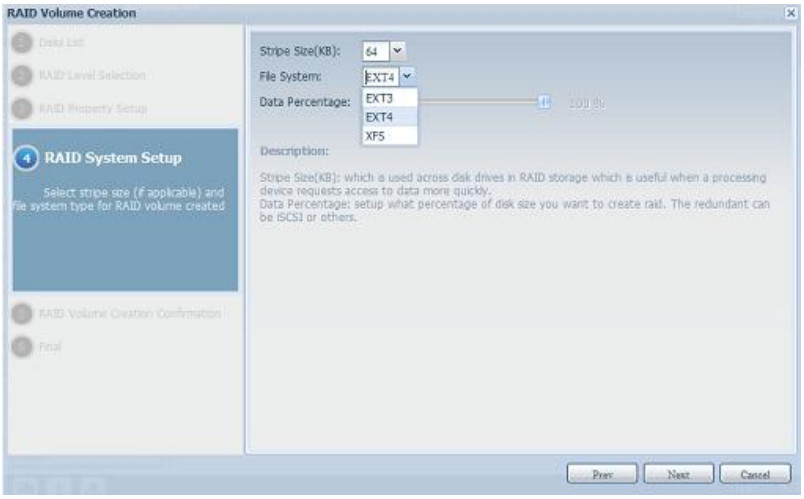


NOTE

We recommend using the "Quick RAID" setting only if the hard disks are brand new or if no existing partitions are contained.

7. Specify a stripe size — 64K is the default setting.

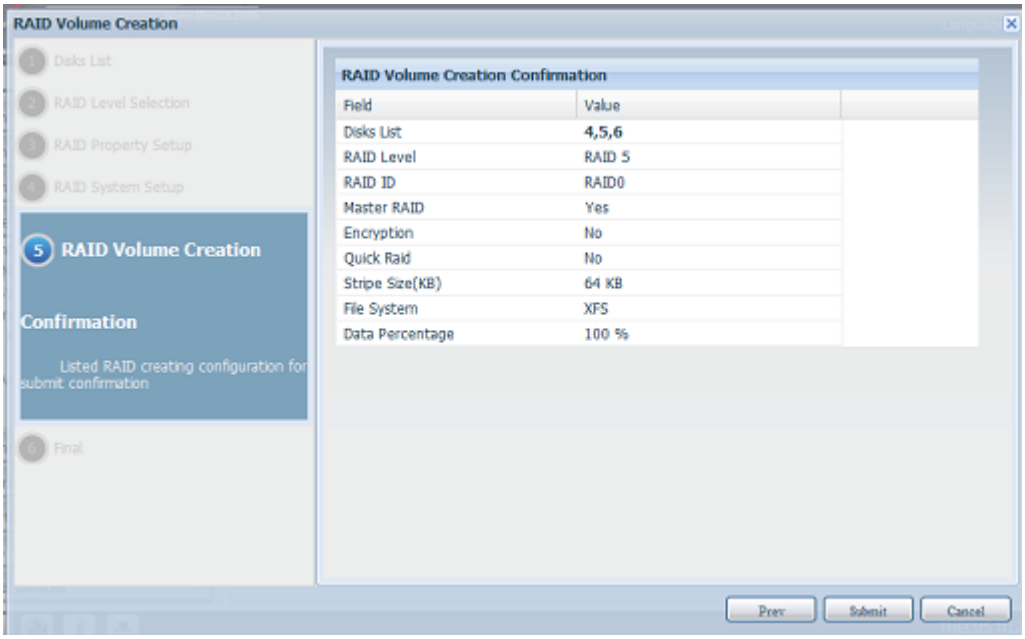
8. Selected the file system you would like to have for this RAID volume. The selection is available from ext3, XFS and ext4.

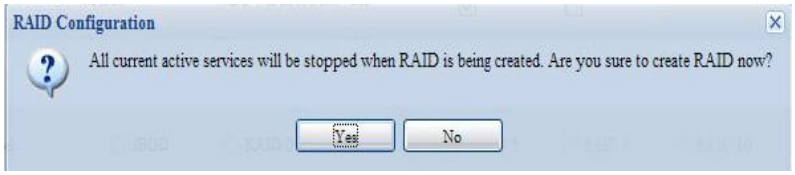


NOTE

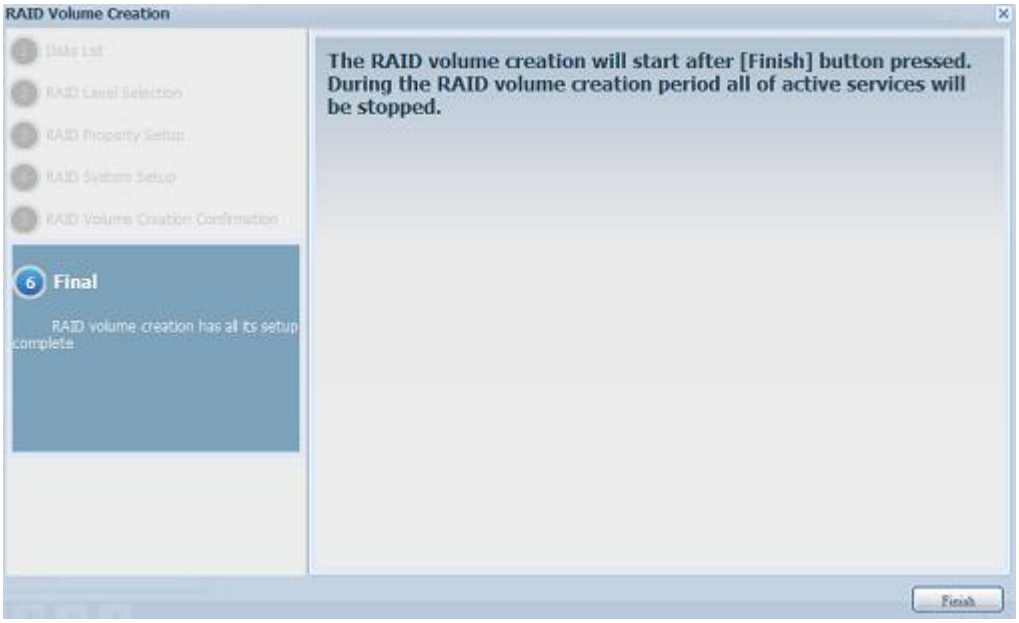
Single volume size supported:
ext3 → 8TB
XFS → 48TB
ext4 → 36TB

9. Press ***Submit*** to build the RAID storage volume.




RAID Configuration
All current active services will be stopped when RAID is being created. Are you sure to create RAID now?
Yes
No

10. Press "Yes" for RAID volume creation preparation. Then click "Finish" to start up with RAID volume building.


RAID Volume Creation
The RAID volume creation will start after [Finish] button pressed. During the RAID volume creation period all of active services will be stopped.
Final
RAID volume creation has all its setup complete
Finish

NOTE Building a RAID volume may be time consuming, depending on the size of hard drives and RAID mode. In general, if the RAID volume building process is up to "RAID Building", then the data volume is accessible.

WARNING Creating RAID destroys all data in the current RAID volume. The data will be unrecoverable.

RAID Level

You can set the storage volume as **JBOD**, **RAID 0**, **RAID 1**, **RAID 5, RAID 6, RAID 10, RAID 50 or RAID 60 (depending on model)**.

Level / Model	JBOD	RAID 0	RAID 1	RAID 5	RAID 6	RAID 10	RAID 50	RAID 60
N12000 series	•	•	•	•	•	•	•	•
N16000 series	•	•	•	•	•	•	•	•
N8900 series	•	•	•	•	•	•	•	•
N6850	•	•	•	•	•	•	•	
N8850	•	•	•	•	•	•	•	•
N10850	•	•	•	•	•	•	•	•
N7700PRO V2	•	•	•	•	•	•	•	
N8800PRO V2	•	•	•	•	•	•	•	•
N5550	•	•	•	•	•	•		
N4510U	•	•	•	•	•	•		
N7510	•	•	•	•	•	•	•	

RAID configuration is usually required only when you first set up the device. A brief description of each RAID setting follows:

RAID Levels	
Level	**Description**
JBOD	The storage volume is a single HDD with no RAID support. JBOD requires a minimum of 1 disk.
RAID 0	Provides data striping but no redundancy. Improves performance

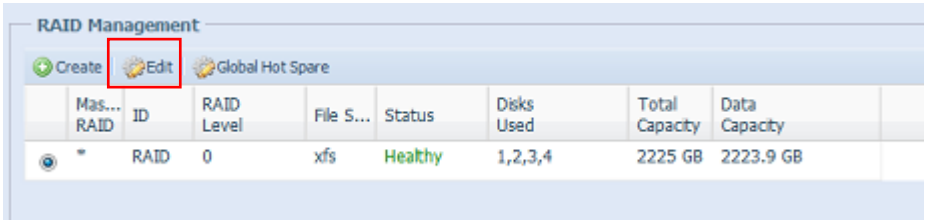
	but not data safety. RAID 0 requires a minimum of 2 disks.
RAID 1	Offers disk mirroring. Provides twice the read rate of a single disk, but same write rate. RAID 1 requires a minimum of 2 disks.
RAID 5	Data striping and stripe error correction information provided. RAID 5 requires a minimum of 3 disks. RAID 5 can sustain one failed disk.
RAID 6	Two independent parity computations must be used in order to provide protection against double disk failure. Two different algorithms are employed to achieve this purpose. RAID 6 requires a minimum of 4 disks. RAID 6 can sustain two failed disks.
RAID 10	RAID 10 has high reliability and high performance. RAID 10 is implemented as a striped array whose segments are RAID 1 arrays. It has the fault tolerance of RAID 1 and the performance of RAID 0. RAID 10 requires 4 disks. RAID 10 can sustain two failed disks.
RAID 50	RAID 50 combines the straight block-level striping of RAID 0 with the distributed parity of RAID 5. This is a RAID 0 array striped across RAID 5 elements. It requires at least 6 drives.
RAID 60	RAID 60 combines the straight block-level striping of RAID 0 with the distributed double parity of RAID 6. That is, a RAID 0 array striped across RAID 6 elements. It requires at least 8 disks.

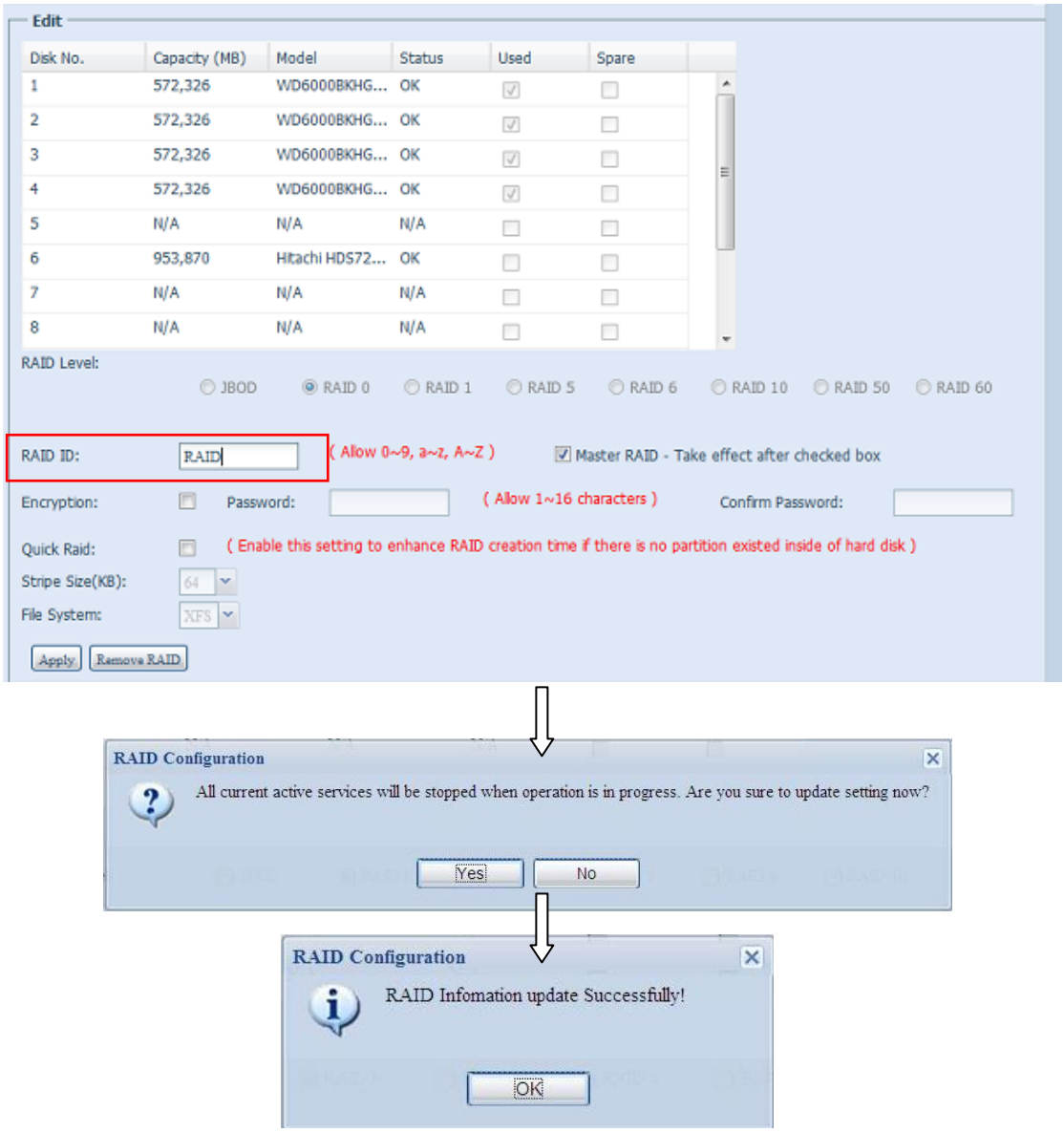
WARNING If the administrator improperly removes a hard disk that should not be removed when RAID status is degraded, all data will be lost.

Edit RAID

On the **RAID Information** screen, press the ***Edit*** button to go to the **RAID Information** screen.

Using **Edit RAID**, you can select RAID ID and the Spare Disk.





Remove RAID

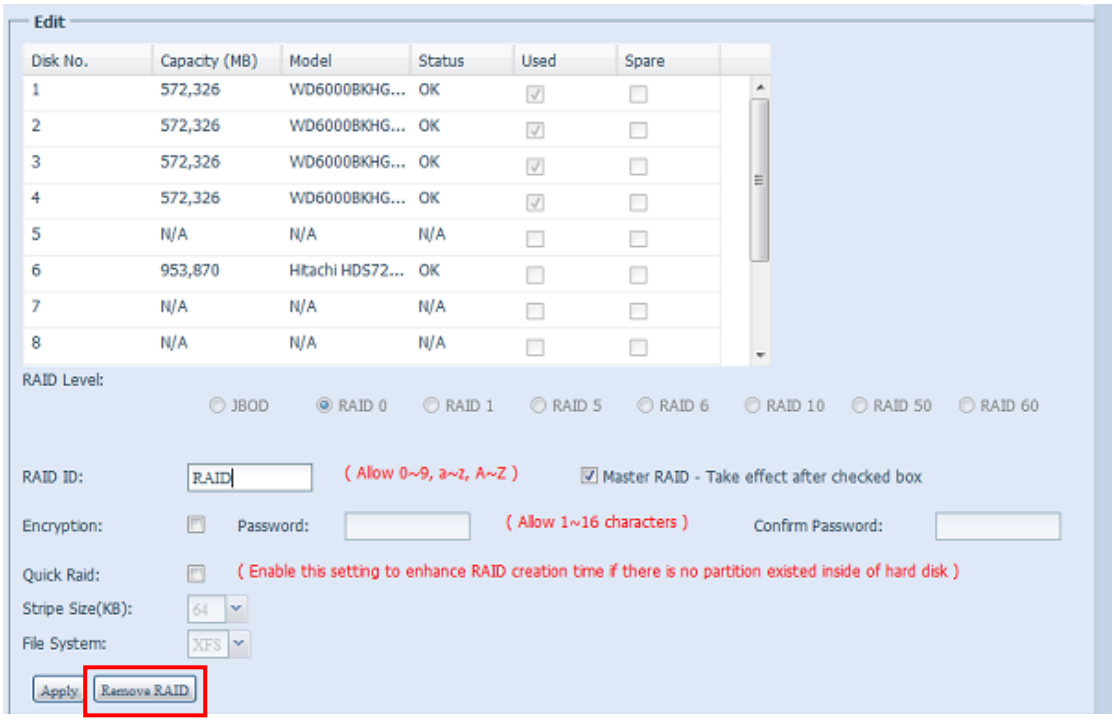
Click to remove the RAID volume. All user data and iSCSI created in the selected RAID volume will be deleted.

To remove a RAID volume, follow the steps below:

1. On the RAID List screen, select the RAID volume by clicking on its radio button, and click ***RAID Information*** to open the **RAID Configuration** screen.

2. On the **RAID Configuration** screen, click ***Remove RAID***.

3. A confirmation screen will appear, you will have to click "Yes" to complete the "**Remove RAID**" operation.

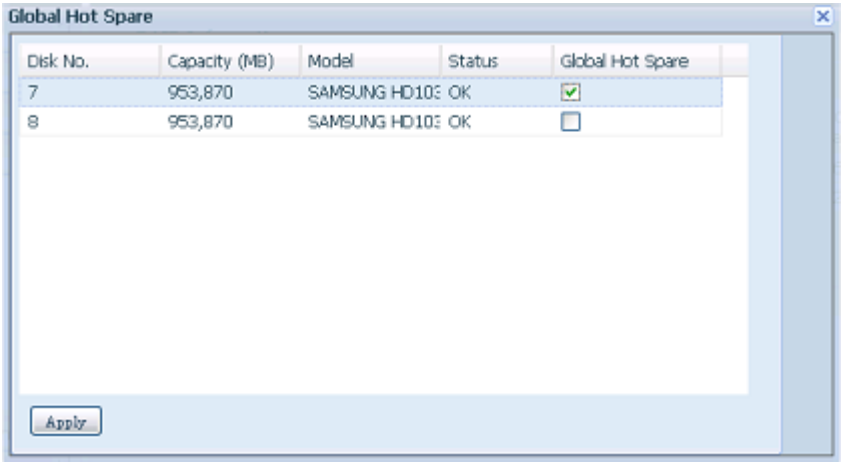


WARNING

Remove RAID destroys all data in the selected RAID volume. The data will be unrecoverable.

Global Hot Spare

Up to 5 RAID volumes can be created per system. The global hot spare support can eliminate the redundant disk usage in each RAID volume. Simply select an unused disk from the global hot spare disk list then apply to activate.



Expanding a RAID

To expand a RAID 1, RAID 5, or RAID 6 volume, follow the steps below:

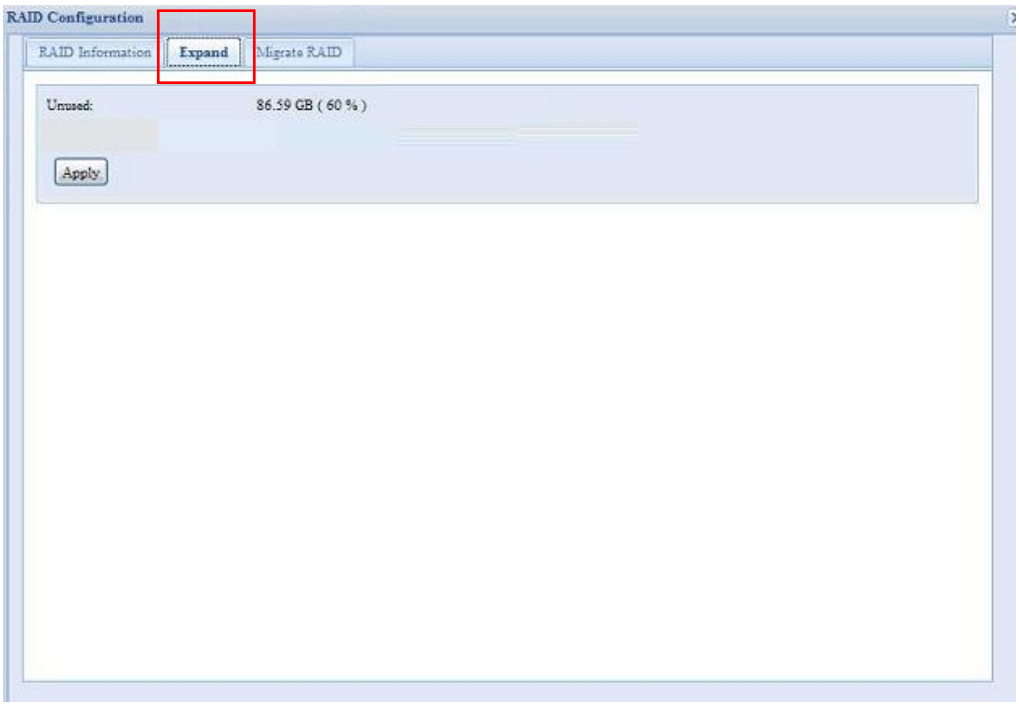
1. Replace one of the hard drives in the RAID volume and allow it to automatically rebuild.

2. Once rebuilt, you can continue to replace any remaining disks in the RAID array.

3. When you are done replacing hard drives, log on to Web Management. Navigate to **Storage**> ***RAID*** to open the **RAID Configuration** screen.

4. On the **RAID Information** screen, click ***Edit*** to open the **RAID Configuration** screen.

5. On the **RAID Configuration** screen, click ***Expand***.



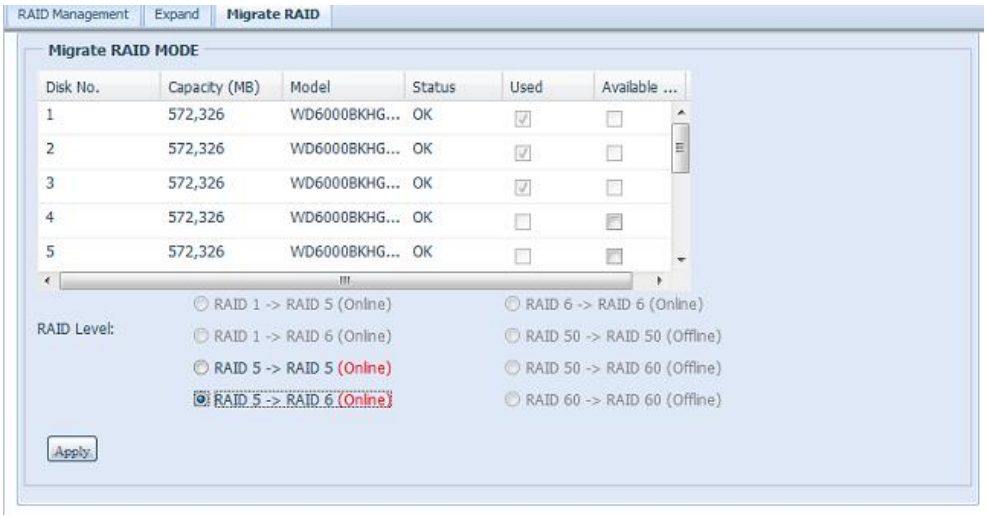
Migrating a RAID

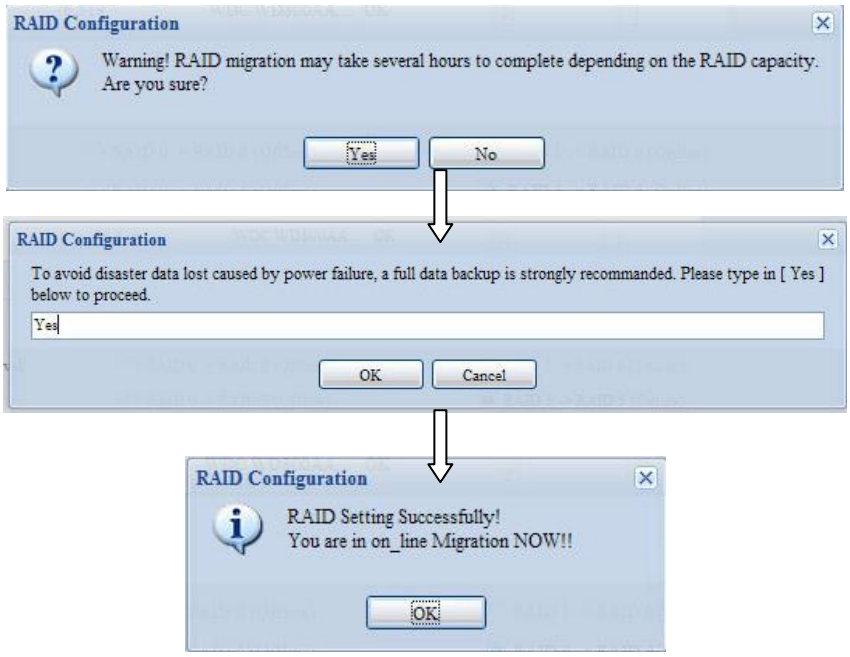
Once a RAID volume has been created, you may want to move it to other physical drives or change the RAID array all together. To migrate a RAID 1, RAID 5, RAID 6, RAID50 or RAID 60 volume, follow the steps below:

1. From the RAID Configuration screen, click **Migrate RAID.**

2. A list of possible RAID migration configurations will be listed. Select the desired migration scheme and click **Apply**.

3. The system will begin migrating the RAID volume.




RAID Configuration
Warning! RAID migration may take several hours to complete depending on the RAID capacity.
Are you sure?
Yes
No
RAID Configuration
To avoid disaster data lost caused by power failure, a full data backup is strongly recommanded. Please type in [Yes] below to proceed.
Yes
OK
Cancel
RAID Configuration
RAID Setting Successfully!
You are in on_line Migration NOW!!
OK

NOTE

- Migrating a RAID volume could take several hours to complete
- The RAID migration feature is available only when it is configurable.

Here is a list of limitation with RAID level migration function:

1. During RAID level migration, it is not permitted to reboot or shutdown system.
2. For RAID migration from **R1 to R5 or R1 to R6**, all services will restart and "iSCSI" volume will be in read only mode but read/write of the "user data" will be possible during the operation.

NOTE

The migration scheme below is based on Thecus IP Storage product's maximum possible combination. For other model which supports less HDD, please refer to the web UI while RAID migration operates.

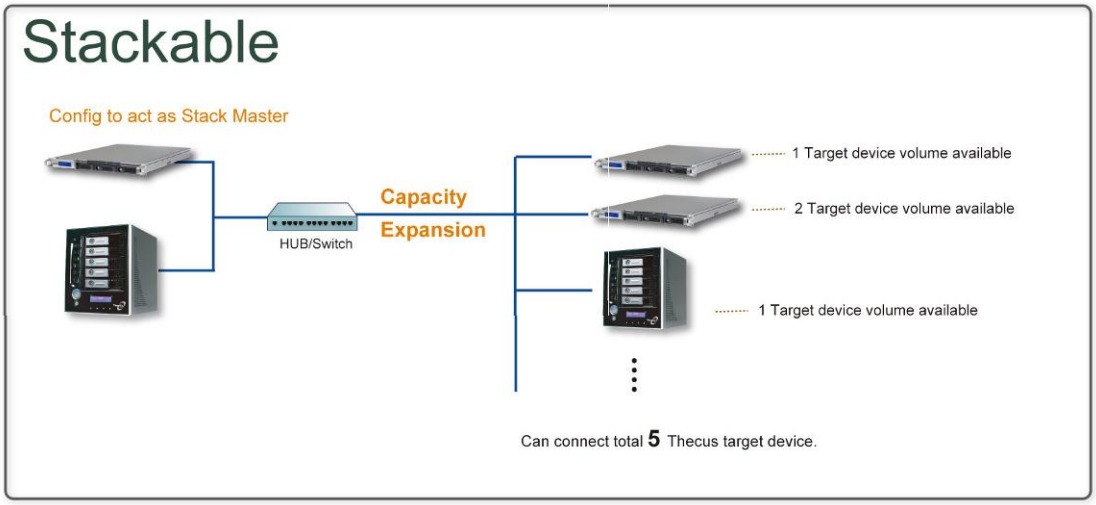
Below is a table listing of possible RAID migration schemes:

To From	RAID 0	RAID 5	RAID 6
RAID 1		[RAID 1] HDDx2 to [RAID 5] HDDx3 [RAID 1] HDDx2 to [RAID 5] HDDx4 [RAID 1] HDDx2 to [RAID 5] HDDx5 [RAID 1] HDDx2 to [RAID 5] HDDx6 [RAID 1] HDDx2 to [RAID 5] HDDx7 [RAID 1] HDDx2 to [RAID 5] HDDx8 ……..HDDx16 [RAID 1] HDDx3 to [RAID 5] HDDx4 [RAID 1] HDDx3 to [RAID 5] HDDx5 [RAID 1] HDDx3 to [RAID 5] HDDx6 [RAID 1] HDDx3 to [RAID 5] HDDx7 [RAID 1] HDDx3 to [RAID 5] HDDx8 ……..HDDx16 [RAID 1] HDDx4 to [RAID 5] HDDx5 [RAID 1] HDDx4 to [RAID 5] HDDx6 [RAID 1] HDDx4 to [RAID 5] HDDx7 [RAID 1] HDDx4 to [RAID 5] HDDx8 ……..HDDx16 [RAID 1] HDDx5 to [RAID 5] HDDx6 [RAID 1] HDDx5 to [RAID 5] HDDx7 [RAID 1] HDDx5 to [RAID 5] HDDx8 ……..HDDx16 [RAID 1] HDDx6 to [RAID 5] HDDx7 [RAID 1] HDDx6 to [RAID 5] HDDx8 ……..HDDx16 [RAID 1] HDDx7 to [RAID 5] HDDx8 ……..HDDx16	[RAID 1] HDDx2 to [RAID 6] HDDx4 [RAID 1] HDDx2 to [RAID 6] HDDx5 [RAID 1] HDDx2 to [RAID 6] HDDx6 [RAID 1] HDDx2 to [RAID 6] HDDx7 [RAID 1] HDDx2 to [RAID 6] HDDx8 ……..HDDx16 [RAID 1] HDDx3 to [RAID 6] HDDx4 [RAID 1] HDDx3 to [RAID 6] HDDx5 [RAID 1] HDDx3 to [RAID 6] HDDx6 [RAID 1] HDDx3 to [RAID 6] HDDx7 [RAID 1] HDDx3 to [RAID 6] HDDx8 ……..HDDx16 [RAID 1] HDDx4 to [RAID 6] HDDx5 [RAID 1] HDDx4 to [RAID 6] HDDx6 [RAID 1] HDDx4 to [RAID 6] HDDx7 [RAID 1] HDDx4 to [RAID 6] HDDx8 ……..HDDx16 [RAID 1] HDDx5 to [RAID 6] HDDx6 [RAID 1] HDDx5 to [RAID 6] HDDx7 [RAID 1] HDDx5 to [RAID 6] HDDx8 ……..HDDx16 [RAID 1] HDDx6 to [RAID 6] HDDx7 [RAID 1] HDDx6 to [RAID 6] HDDx8 ……..HDDx16 [RAID 1] HDDx7 to [RAID 6] HDDx8 ……..HDDx16
RAID 5	X	[RAID 5] HDDx3 to [RAID 5] HDDx4 [RAID 5] HDDx3 to [RAID 5] HDDx5 [RAID 5] HDDx3 to [RAID 5] HDDx6 [RAID 5] HDDx3 to [RAID 5] HDDx7 [RAID 5] HDDx3 to [RAID 5] HDDx8 ……..HDDx16 [RAID 5] HDDx4 to [RAID 5] HDDx5 [RAID 5] HDDx4 to [RAID 5] HDDx6 [RAID 5] HDDx4 to [RAID 5] HDDx7 [RAID 5] HDDx4 to [RAID 5] HDDx8 ……..HDDx16 [RAID 5] HDDx5 to [RAID 5] HDDx6 [RAID 5] HDDx5 to [RAID 5] HDDx7 [RAID 5] HDDx5 to [RAID 5] HDDx8 ……..HDDx16 [RAID 5] HDDx6 to [RAID 5] HDDx7 [RAID 5] HDDx6 to [RAID 5] HDDx8 ……..HDDx16 [RAID 6] HDDx7 to [RAID 5] HDDx8 ……..HDDx16	[RAID 5] HDDx3 to [RAID 6] HDDx5 [RAID 5] HDDx3 to [RAID 6] HDDx6 [RAID 5] HDDx3 to [RAID 6] HDDx7 [RAID 5] HDDx3 to [RAID 6] HDDx8 ……..HDDx16 [RAID 5] HDDx4 to [RAID 6] HDDx6 [RAID 5] HDDx4 to [RAID 6] HDDx7 [RAID 5] HDDx4 to [RAID 6] HDDx8 ……..HDDx16 [RAID 5] HDDx5 to [RAID 6] HDDx7 [RAID 5] HDDx5 to [RAID 6] HDDx8 ……..HDDx16 [RAID 5] HDDx6 to [RAID 6] HDDx8 ……..HDDx16

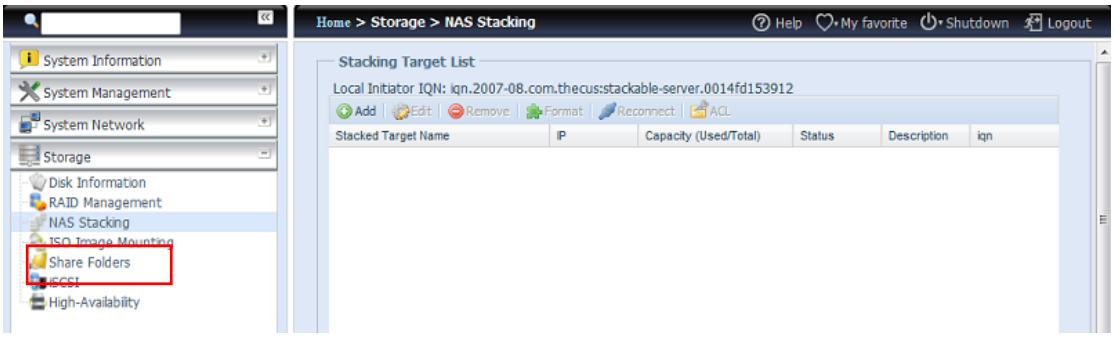
RAID 6	X	X	[RAID 6] HDDx4 to [RAID 6] HDDx5 [RAID 6] HDDx4 to [RAID 6] HDDx6 [RAID 6] HDDx4 to [RAID 6] HDDx7 [RAID 6] HDDx4 to [RAID 6] HDDx8 ……..HDDx16 [RAID 6] HDDx5 to [RAID 6] HDDx6 [RAID 6] HDDx5 to [RAID 6] HDDx7 [RAID 6] HDDx5 to [RAID 6] HDDx8 ……..HDDx16 [RAID 6] HDDx6 to [RAID 6] HDDx7 [RAID 6] HDDx6 to [RAID 6] HDDx8 ……..HDDx16 [RAID 6] HDDx7 to [RAID 6] HDDx8 ……..HDDx16

NAS Stacking

The Thecus IP storage's capacity can be expanded even further using the stackable function. With it, users can expand the capacity of their network storage systems up to 5 other stack target volumes which are located in different systems. These can be stacked through single network access like SMB or AFP acting as a share folder type.



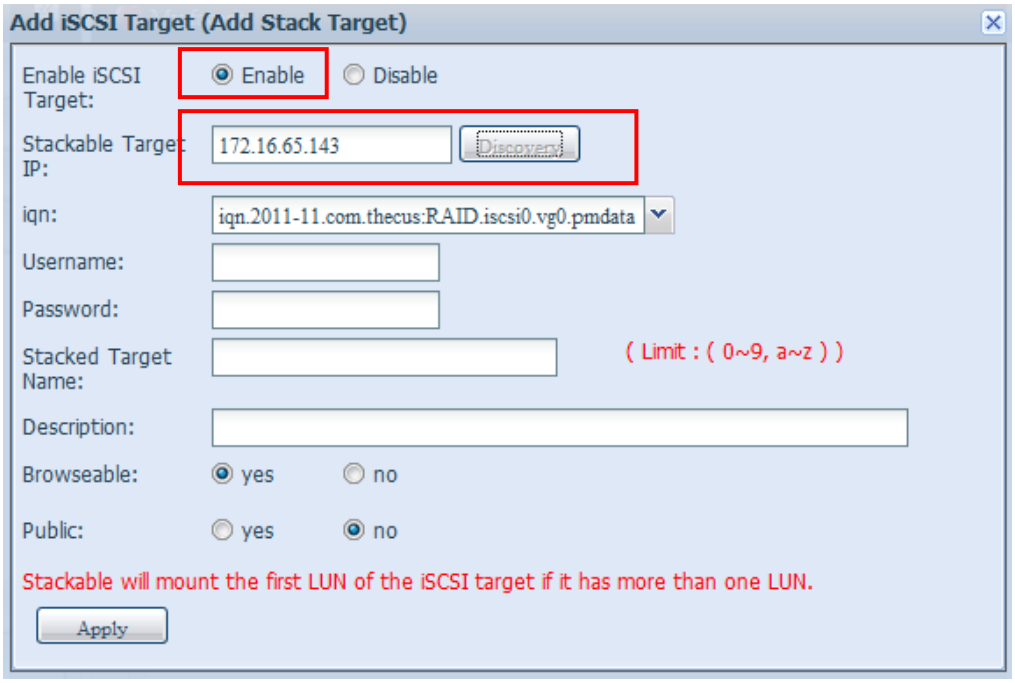
From the main menu, the stackable feature is located under "Storage". Please refer the figure below for reference.



A. *Add a Stack Target Volume*

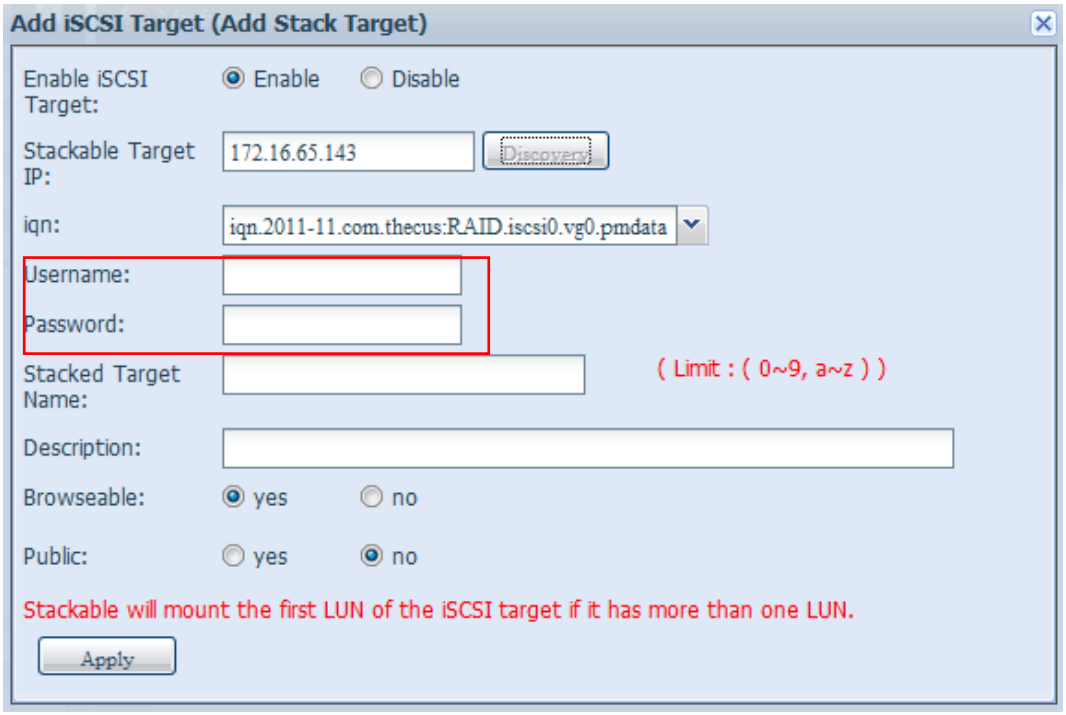
From the figure above, click ***Add*** to access the stackable target device configuration page. Please refer to the figure below:

With the added stack target you can "Enable" or "Disable" the stack target now or later depending on usage required.

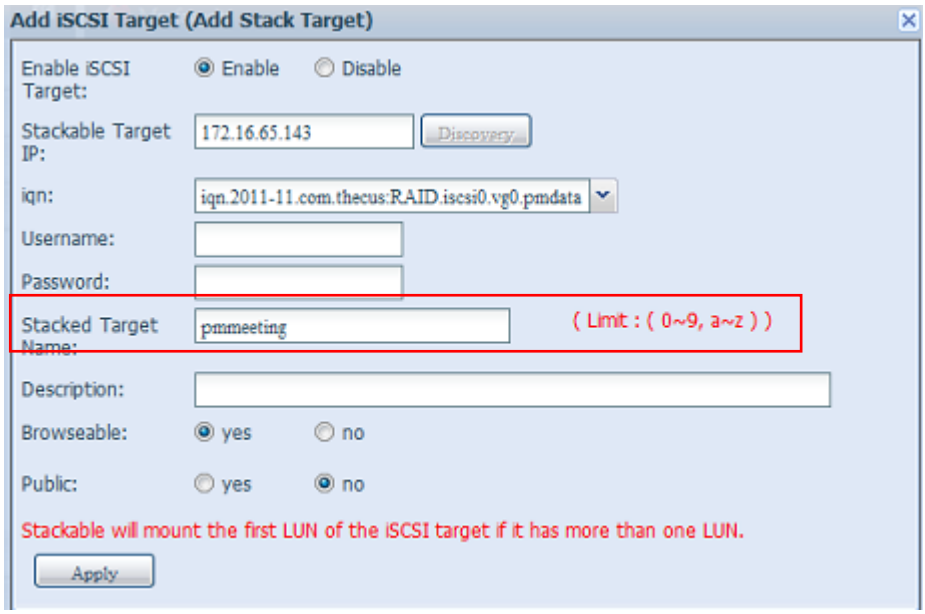


Next, input the target IP address of the stackable device and click the ***Discovery*** button. The system will list available target volumes from the inputted IP address.

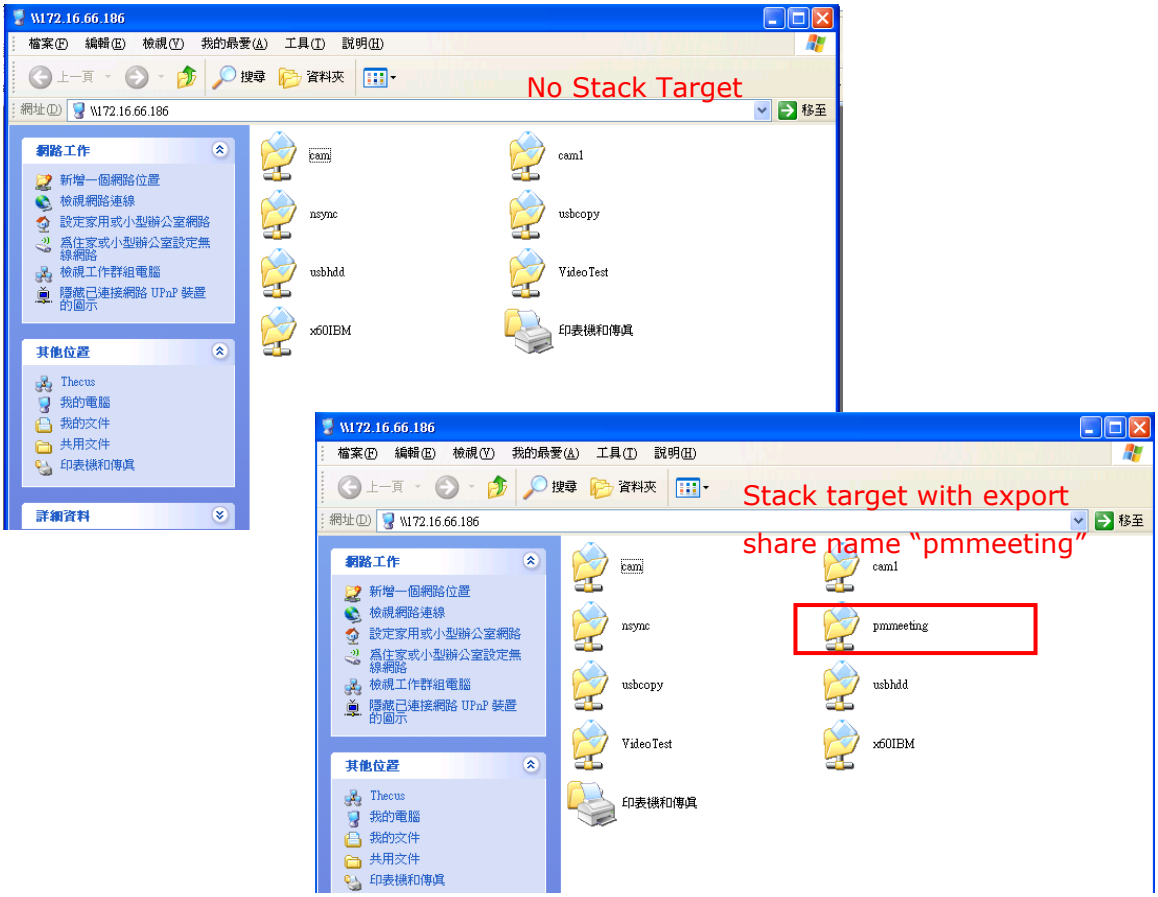
Once the volume IP has been set, you may need to input a valid user name and password to validate your access rights. If there is no user name and password needed to access target volume, then leave it blank.



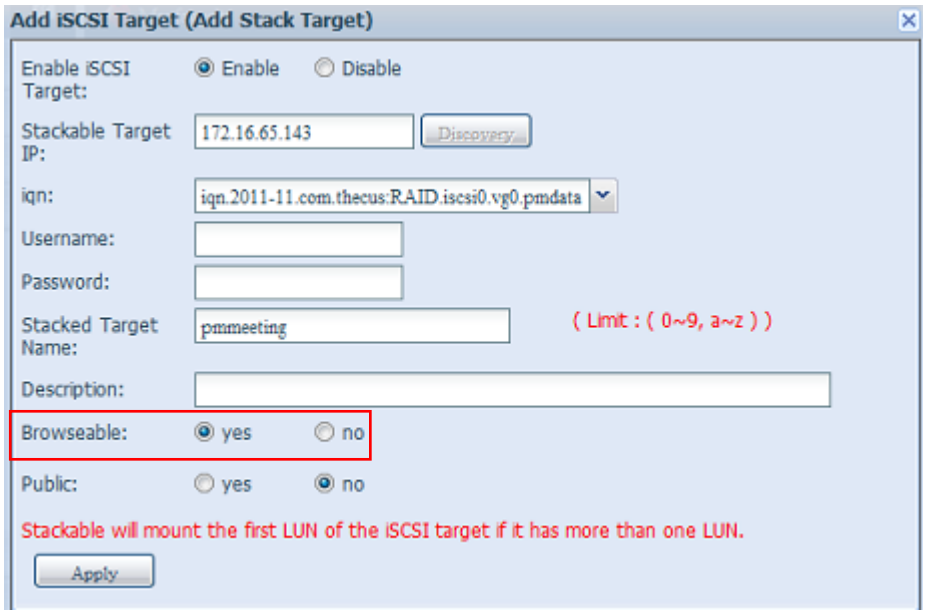
The **Stacked Target name** will become the network share name and will be displayed through network access such as SMB. You may refer to the figure below to see the result. Please note the naming limitation.



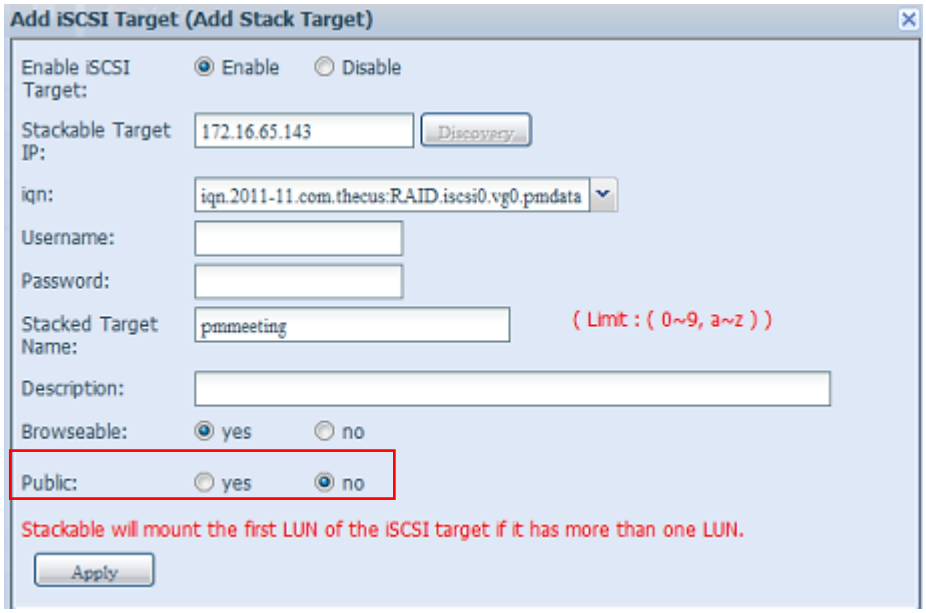
From the figure above, the **Stacked Target name** is "pmmeeting". The figures below show the result before and after via Microsoft Network Access when settings have been completed.



The **Browseable** setting is the same method used for setting a system share folder. It designates whether or not this folder will be visible through web disk. You may refer to the figure below for reference when **Yes** and **No** are selected.



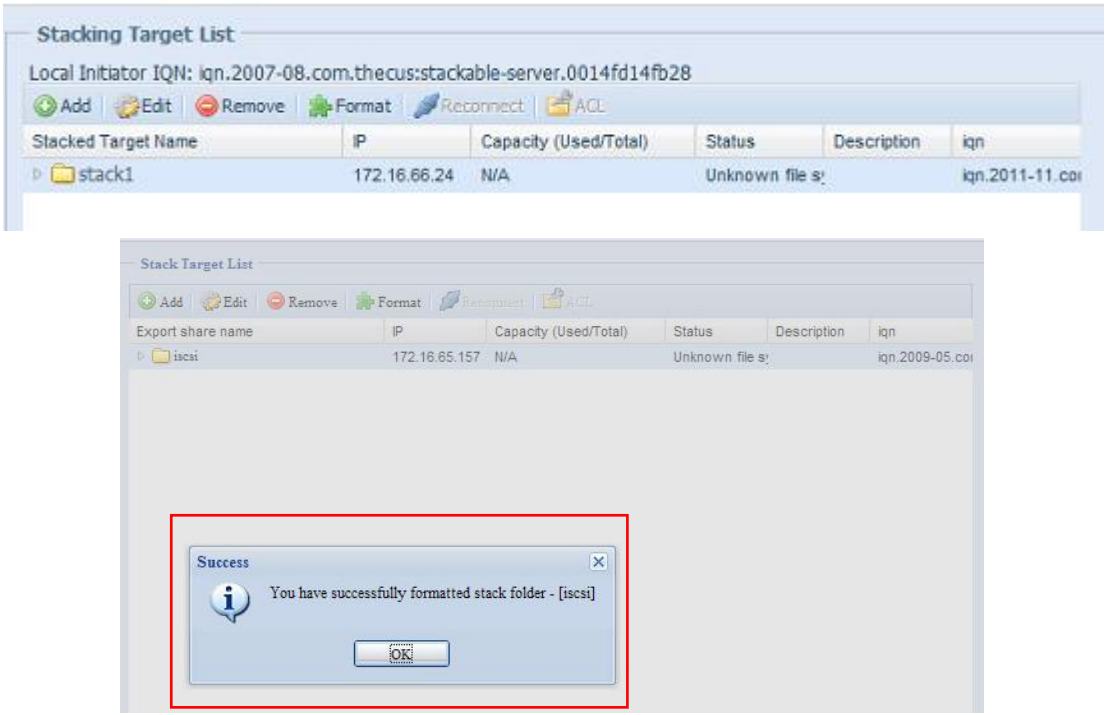
The **Public** setting will be set the same way as the setting for the system share folder associated with the ACL permission is. If **Public** is set to **Yes**, all users will be able to access it, and **ACL** button will be grayed out. If **Public** is set to **No**, the ACL button will be available in the **Stack Target List** window.



Click ***Apply*** to save your changes.

B. Activate a Stack Target

After your settings have been applied, the system will bring you back to the **Stack Target List** window as shown below. There is one stack target device that has been attached into this stack master.

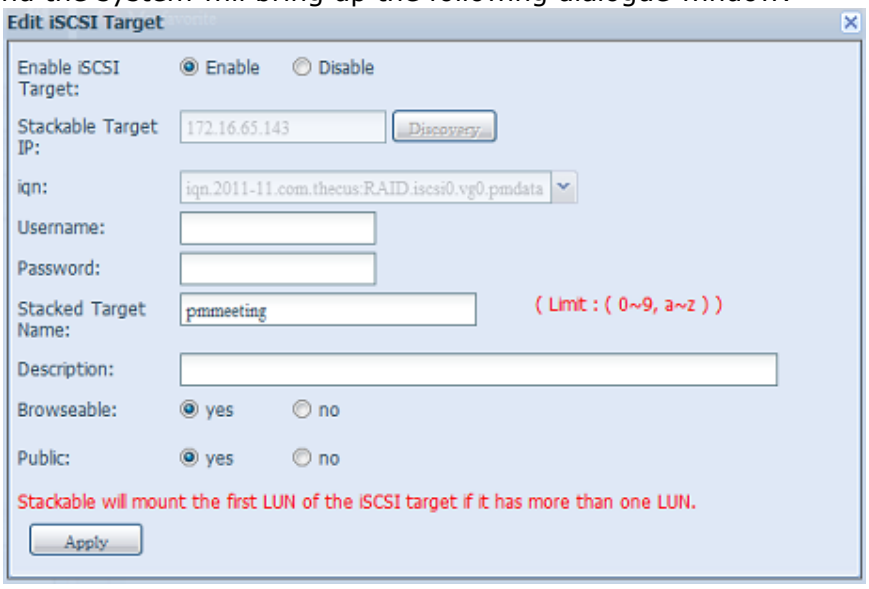


With this newly attached stack target device, you will see the information displayed and also have access to several options to choose from.

In general, if the attached stack target device has been used by another Thecus NAS as stack target volume, then the **Format** item will be display and system will recognize it straight away and display its capacity. Otherwise, the **Format** item will be available and the **Capacity** and **Status** items will show as "`N/A`" and "`Unknown file system`" respectively.
Next, click ***Format*** to proceed with formatting.
After the format is completed, the stack target volume will be created successfully. You will see the volume's capacity and status in the **Stack Target List** screen.

C. *Edit a Stack Target*

To make any changes to a stack target, click ***Edit*** for the corresponding stack target, and the system will bring up the following dialogue window:

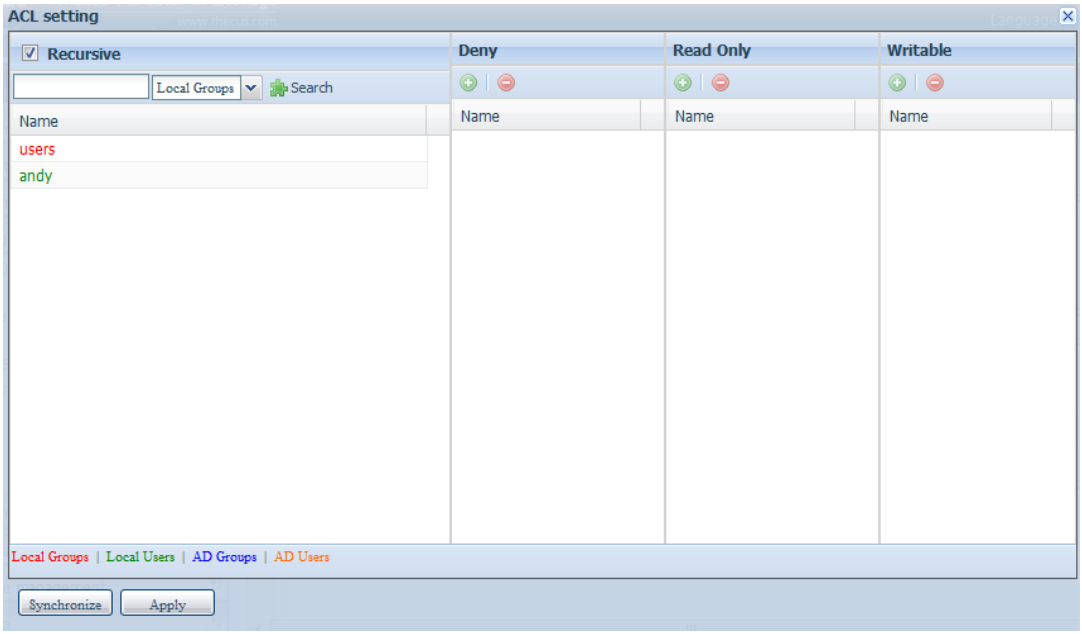


After your changes have been made, click ***Apply*** to confirm any modifications. Once changes are applied, the associated information will be updated on the **Stack Target List** window.

D. *Stack Target ACL*

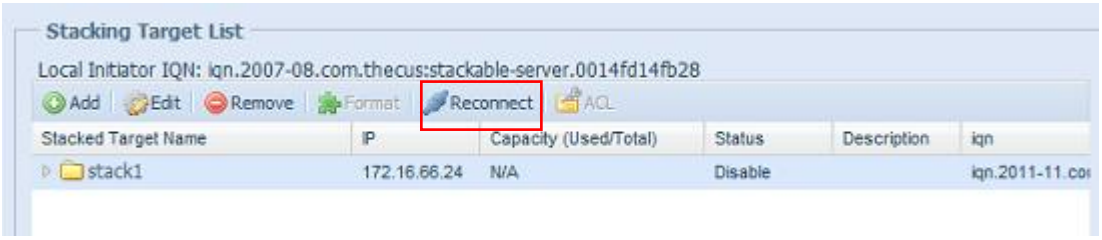
If the stack target **Public** setting set to ***Yes***, then the **ACL** button will be grayed out. However, if **Public** setting is set to ***No***, then the **ACL** button will be available for you to setup user access permissions for the stack target.

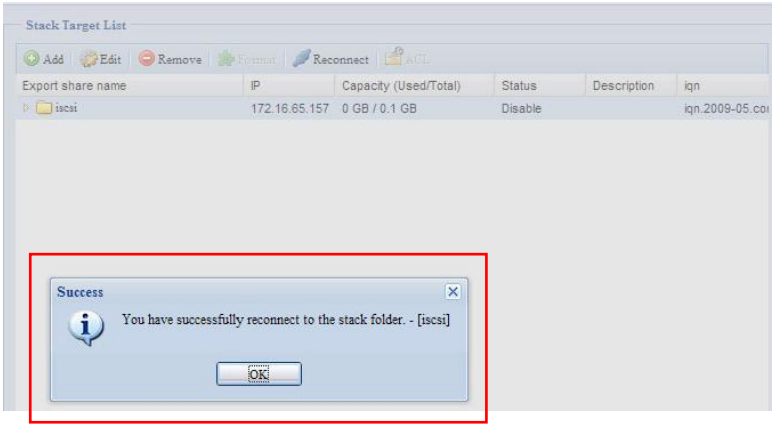
The **ACL** settings will be exactly the same as the system folder that you may have setup previously.



E. *Reconnect a Stack Target*

This is used to enable stack target devices that may have been disconnected due to a power outage or a disconnected network. When this happens, the **Reconnect** button will become available. To attempt to reconnect the stack target, click ***Reconnect***.



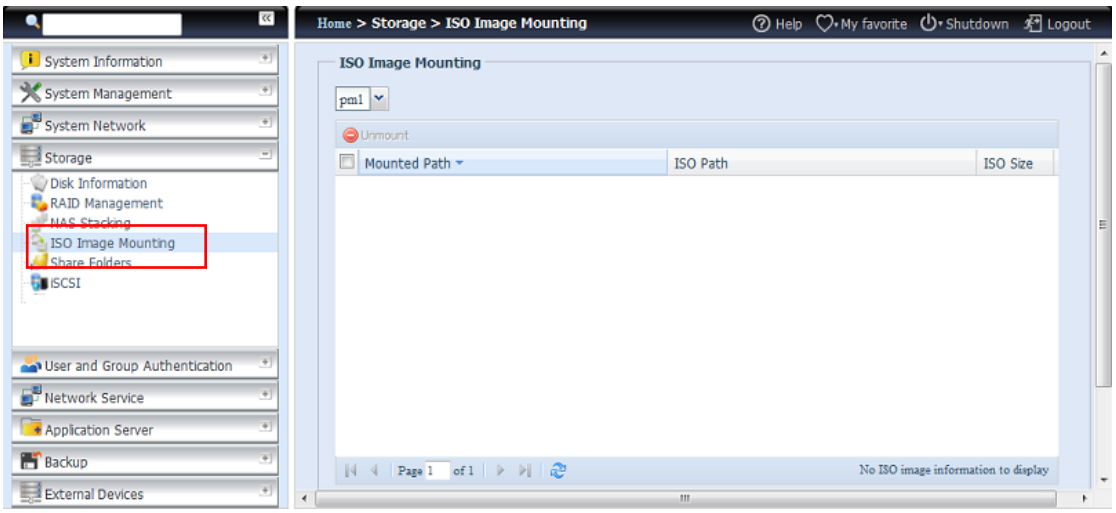


ISO Mount

The ISO Mount feature is a very useful tool from the Thecus products. With it, users can mount an ISO file and have the export name display all the details from the mounted ISO file.

From the main menu, the ISO Mount feature is located under "Storage". Please refer the figure below for reference.

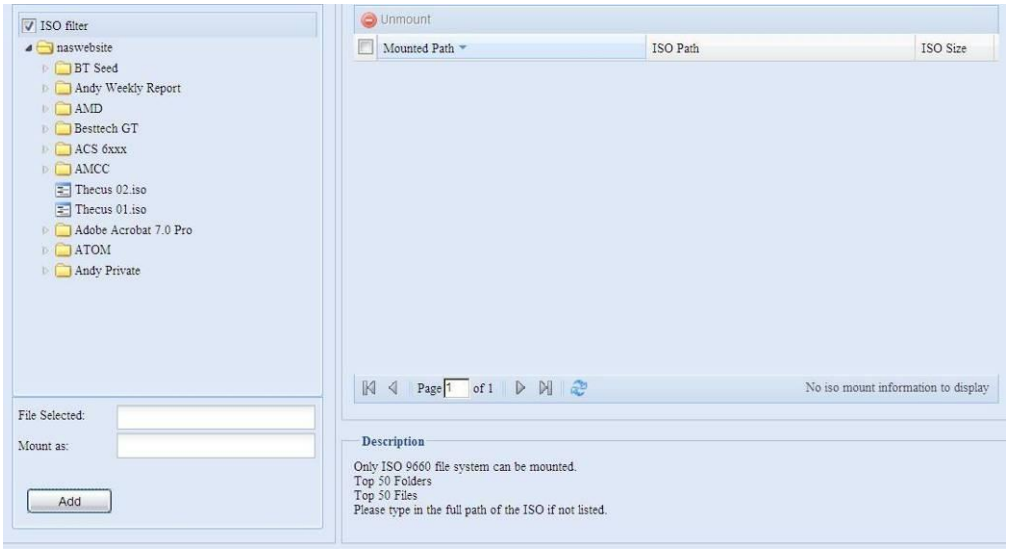
Select the **ISO Image Mounting** function and the ISO Image Mounting window will appear as shown here.

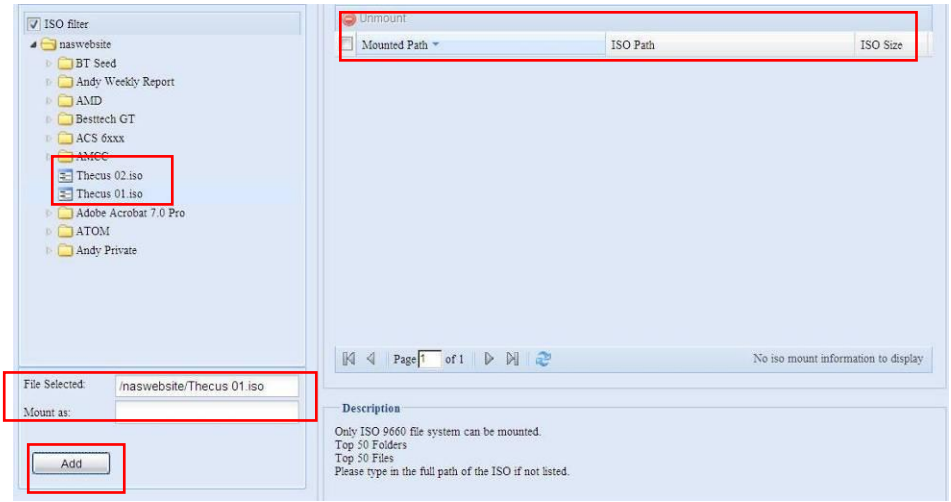


A. *Add an ISO file*

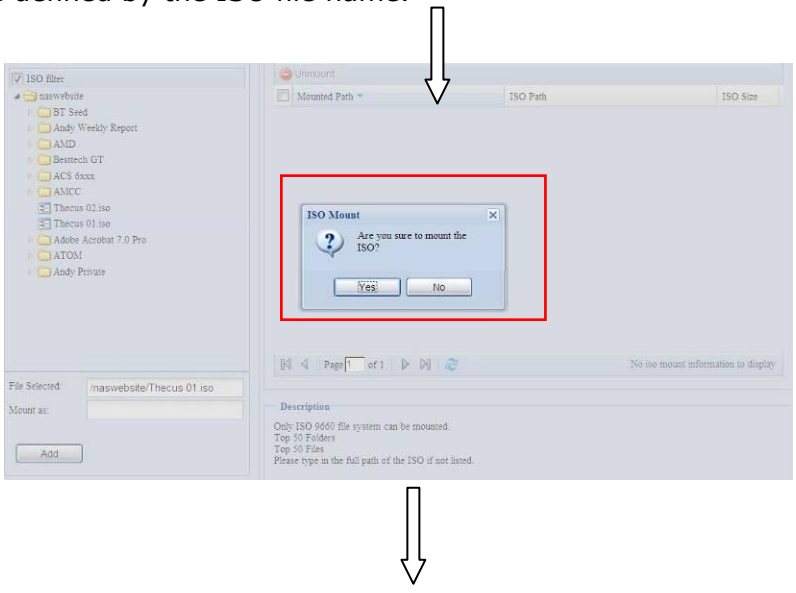
From the figure above, select an ISO file from the drop down share list.

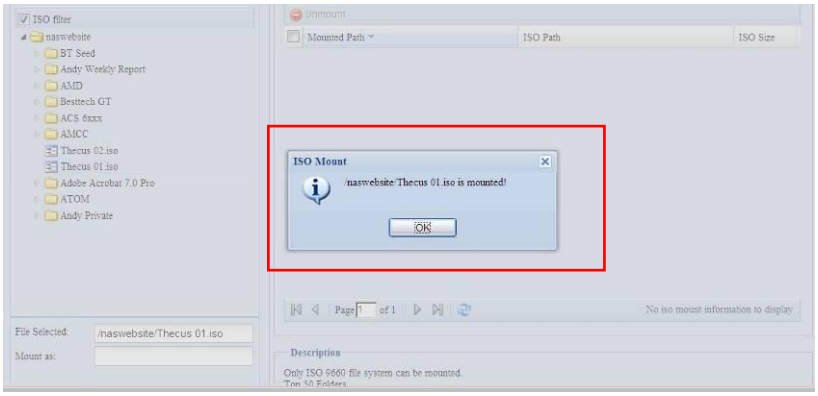
After selection, the system will bring up the Mount table screen for further settings.



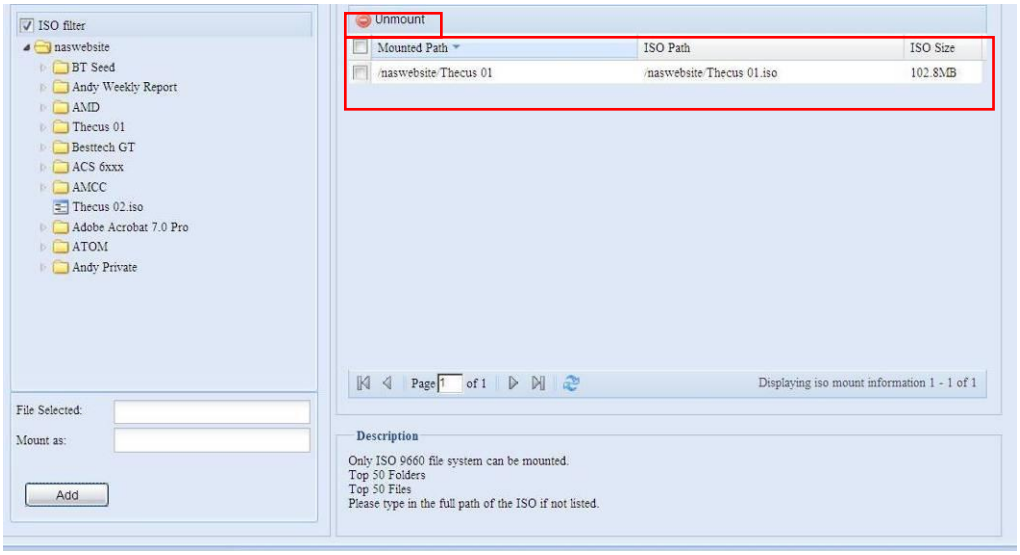


To mount the new ISO file, select one file from the list of files and input the desired mounting name into the "Mount as:" field. Click "ADD" to confirm the completion of the mounting. If nothing is input in the "Mount as" ISO file export name field, the system will automatically give an export name to the ISO file. The mounting name will then be defined by the ISO file name.





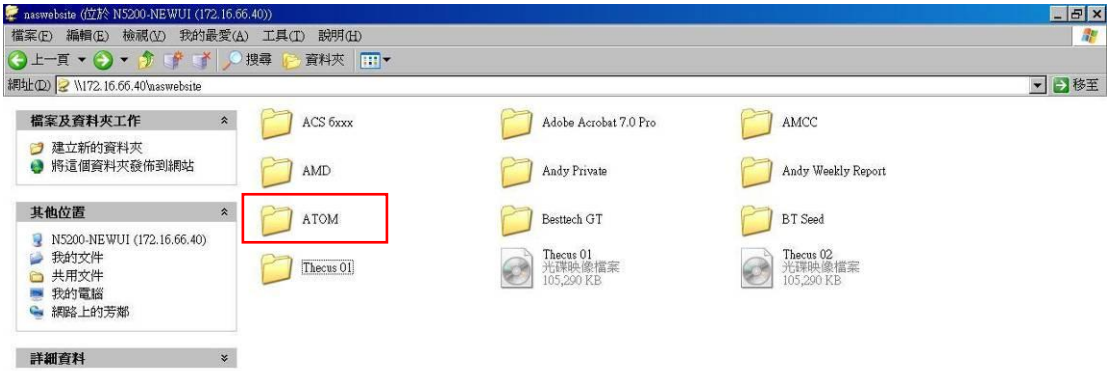
After completion, the page will display all mounted ISO files.



You can click "Unmount" to eliminate a mounted ISO file.

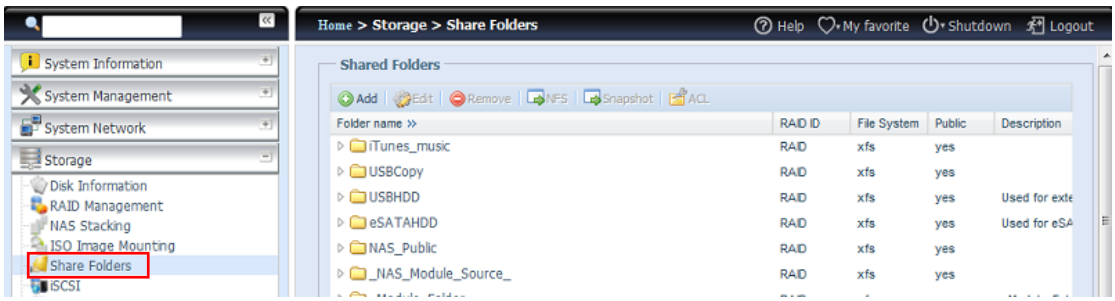
B. *Using ISO*

The mounted ISO file will be located in the share folder of the same name as the file. Please refer the screen shot below. Here, the ISO file "Thecus 01" wasn't assigned a mounting name, so the system automatically created a folder "Thecus 01".



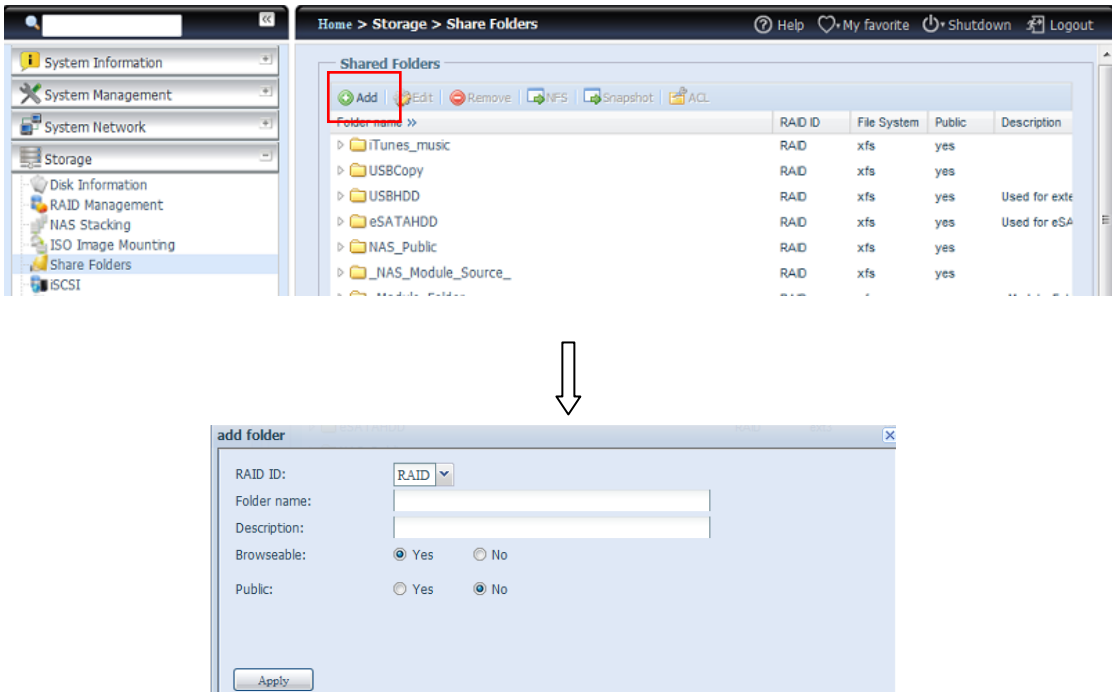
Share Folder

From the **Storage** menu, choose ***Share Folders***, and the **Shared Folder** screen appears. This screen allows you to create and configure folders on the Thecus IP storage volume.



Adding Folders

On the **Folder** screen, press the ***Add*** button and the **Add Folder** screen appears. This screen allows you to add a folder. After entering the information, press ***Apply*** to create new folder.



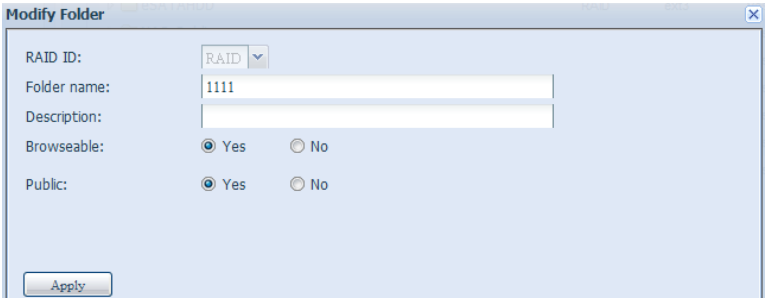
Add Folder	
Item	**Description**
RAID ID	RAID volume where the new folder will reside.
Folder Name	Enter the name of the folder.
Description	Provide a description the folder.
Browseable	Enable or disable users from browsing the folder contents. If **Yes** is selected, then the share folder will be browseable.
Public	Admit or deny public access to this folder. If **Yes** is selected, then users do not need to have access permission to write to this folder. When accessing a public folder via FTP, the behavior is similar to anonymous FTP. Anonymous users can upload/download a file to the folder, but they cannot delete a file from the folder.
Apply	Press ***Apply*** to create the folder.

NOTE

Folder names are limited to 60 characters. Systems running Windows 98 or earlier may not support file names longer than 15 characters.

Modify Folders

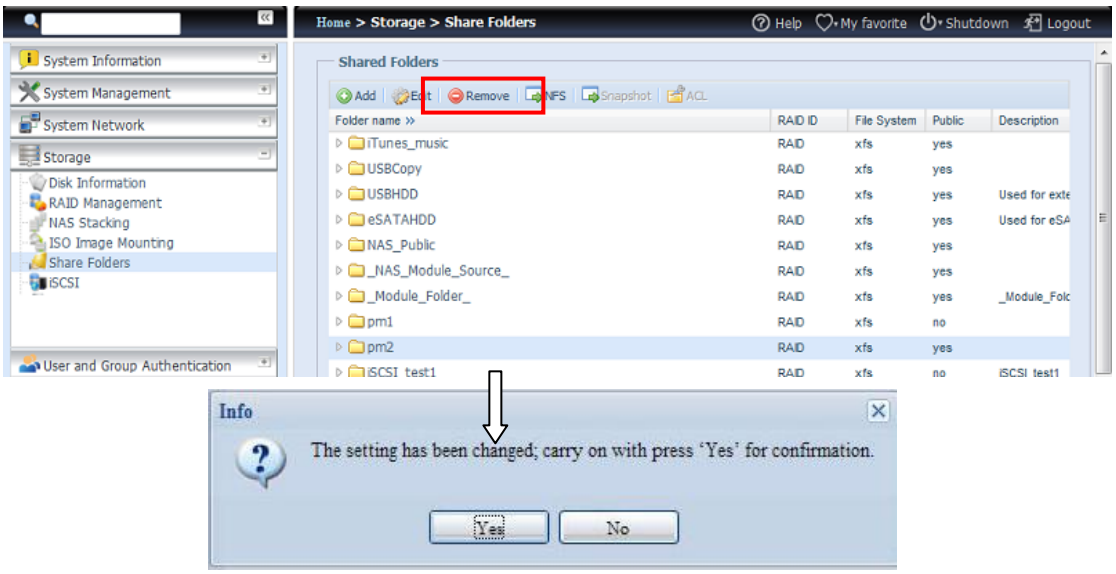
On the **Folder** screen, press the ***Edit*** button and the **Modify Folder** screen appears. This screen allows you to change folder information. After entering the information, press **Apply** to save your changes.



Modify Folder	
Item	**Description**
RAID ID	RAID volume where the folder will reside.
Folder Name	Enter the name of the folder.
Description	Provide a description the folder.
Browseable	Enable or disable users from browsing the folder contents. This setting will only apply while access via SMB/CIFS and web disk.
Public	Admit or deny public access to this folder.

Remove Folders

To remove a folder, press the ***Remove*** button from the specified folder row. The system will confirm folder deletion. Press ***Yes*** to delete the folder permanently or ***No*** to go back to the folder list.

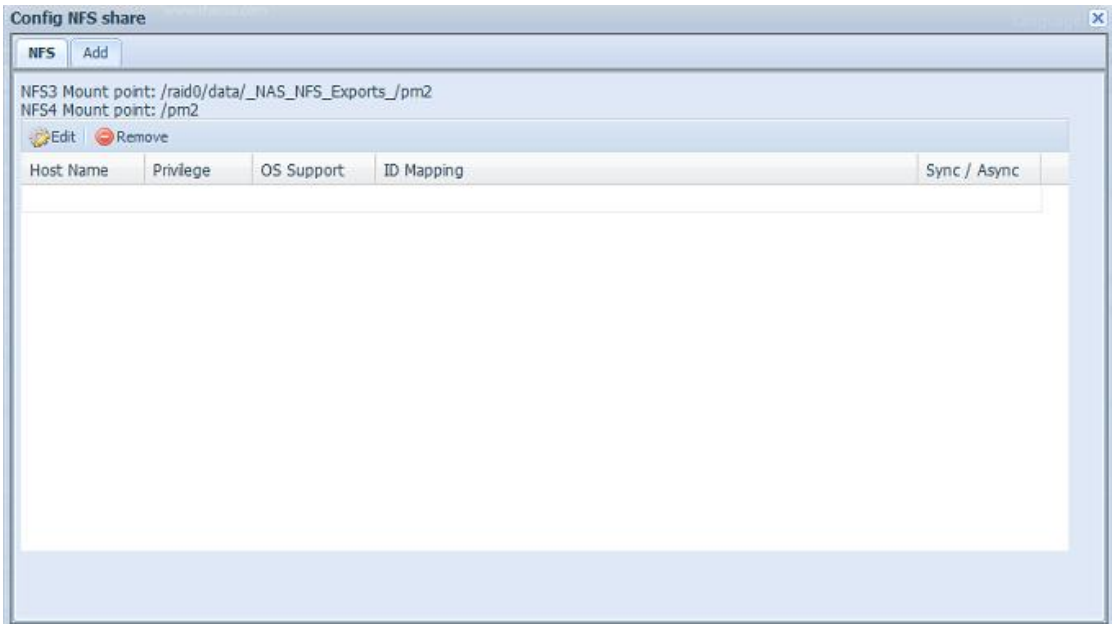


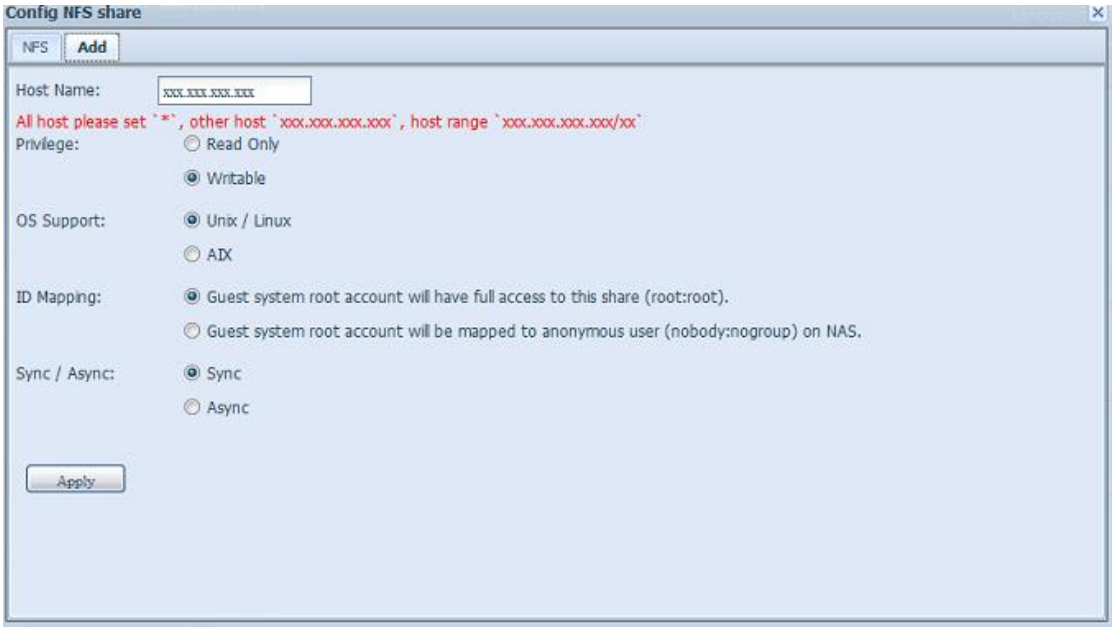
WARNING

All the data stored in the folder will be deleted once the folder is deleted. The data will not be recoverable.

NFS Share

To allow NFS access to the share folder, enable the **NFS Service**, and then set up hosts with access rights by clicking ***Add***.



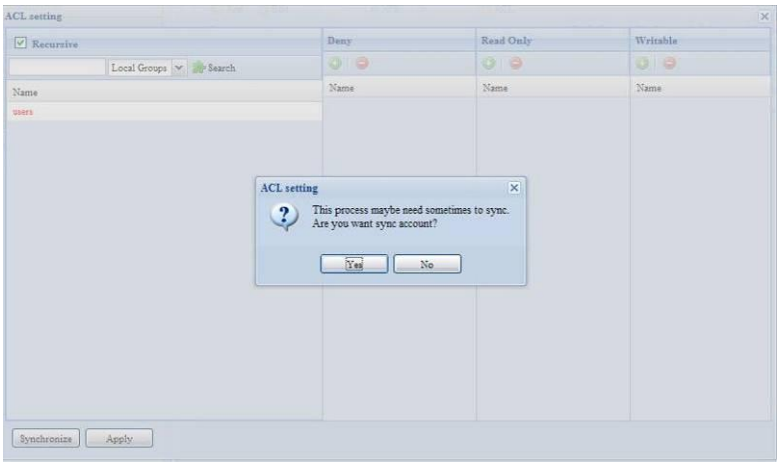


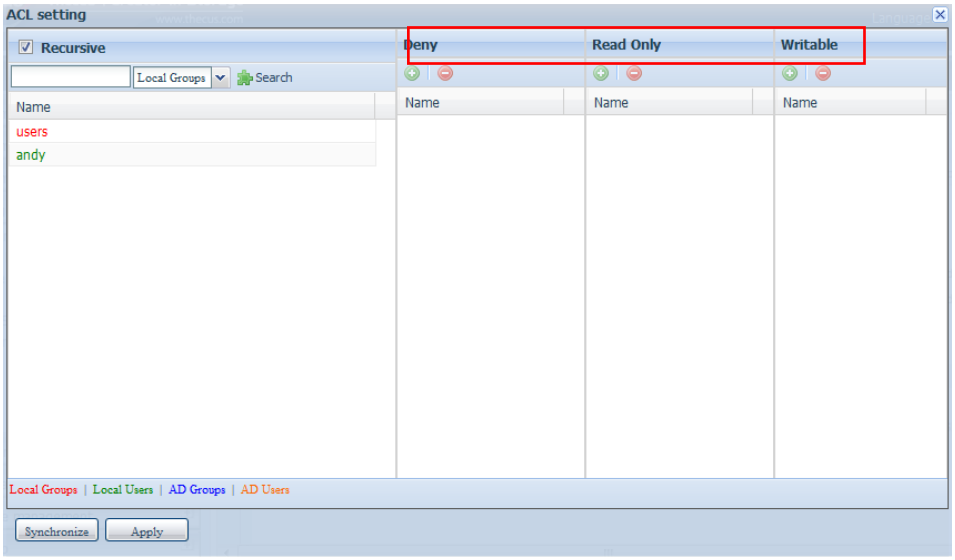
NFS Share	
Item	**Description**
Hostname	Enter the name or IP address of the host
Privilege	Host has either read only or writeable access to the folder.
OS Support	There are two selections available: • Unix / Linux System • AIX (Allow source port > 1024) Choose the one which best fits your needs.
ID Mapping	There are three selections available: • Guest system root account will have full access to this

	share (root:root). • Guest system root account will be mapped to anonymous user (nobody:nogroup) on NAS. • All user on guest system will be mapped to anonymous user (nobody:nogroup) on NAS. Choose the one which best fits your needs.
Sync / Async	Choose to determine the data "Sync" at once or "Async" in arranged batch.
Apply	Click to save your changes.

Folder and sub-folders Access Control List (ACL)

On the Folder screen, press the ***ACL*** button, and the **ACL setting** screen appears. This screen allows you to configure access to the specific folder and sub-folders for users and groups. Select a user or a group from the left hand column and then choose ***Deny***, ***Read Only***, or ***Writable*** to configure their access level. Press the ***Apply*** button to confirm your settings.





ACL setting	
Item	**Description**
Deny	Denies access to users or groups who are displayed in this column.
Read Only	Provides Read Only access to users or groups who are displayed in this column.

Writable	Provides Write access to users or groups who are displayed in this column.
Recursive	Enable to inherit the access right for all its sub-folders.

To configure folder access, follow the steps below:

1. On the **ACL** screen, all network groups and users are listed in the left hand column. Select a group or user from this list.

2. With the group or user selected, press one of the buttons from the three access level columns at the top. The group or user then appears in that column and has that level of access to the folder.

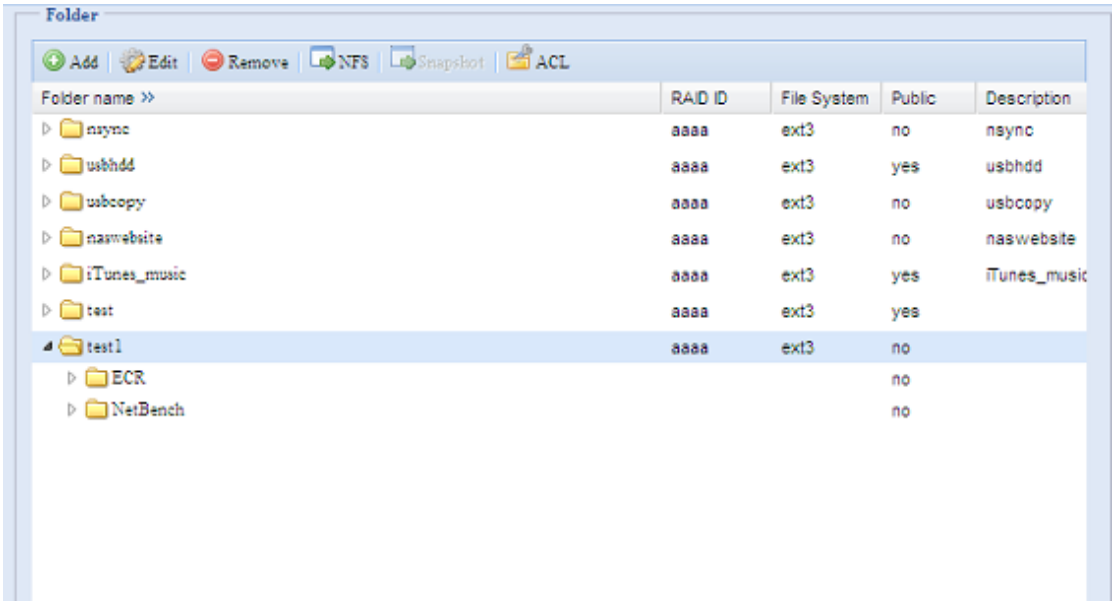
3. Continue selecting groups and users and assigning them access levels using the column buttons.
4. To remove a group or user from an access level column, press the ***Remove*** button in that column.

5. When you are finished, press ***Apply*** to confirm your ACL settings.

NOTE

If one user has belonged to more than one group with different privilege, then the priority of the privilege will be as followed:
Deny > Read Only > Writable

To setup sub-folders ACL, click on " ▷ " symbol to extract sub folders list as screen shot shows below. You may carry on with same steps as share level ACL setting.



NOTE

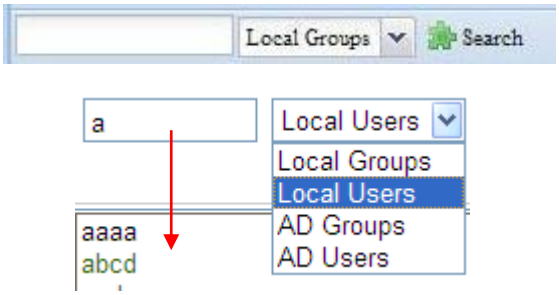
The ACL can only be set for share and sub-folders level, not for files.

The ACL screen also allows you to search for a particular user. To do this, follow the steps below:

1. In the blank, enter the name of the user you would like to find.

2. From the drop down select the group you would like to search for the user in.

3. Click ***Search***.

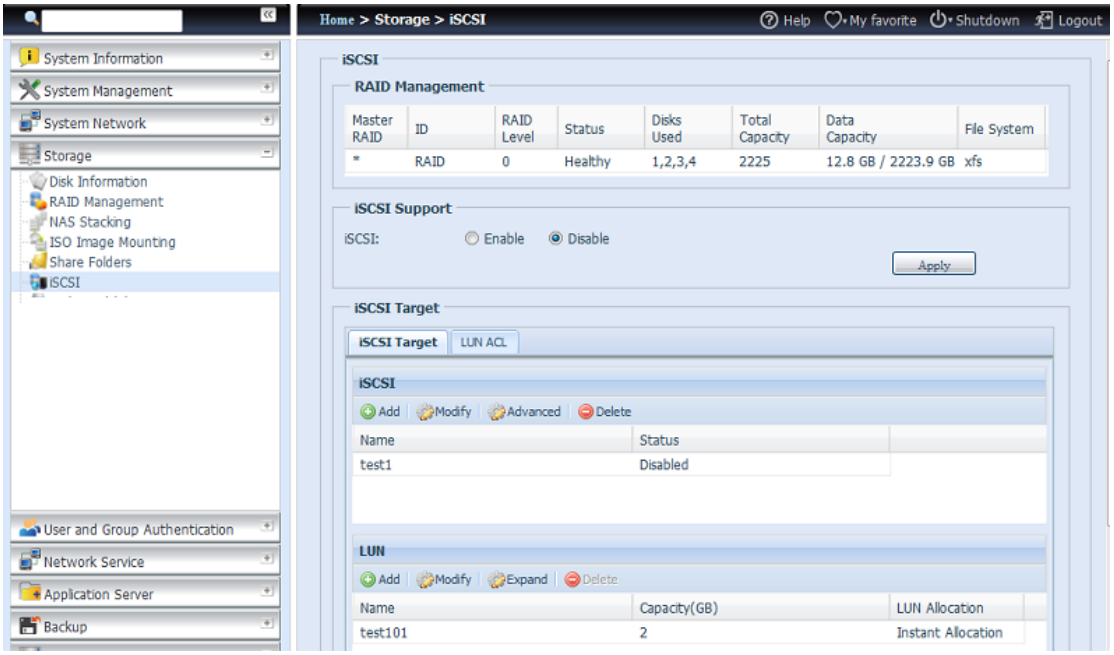


NOTE The system will list up to 1,000 users from the chosen category. To narrow your search, enter a search term in the blank provided.

iSCSI

You may specify the space allocated for iSCSI. See the table below to the allowed iSCSI target number per system:

Model	N8900V N6850 N5550 N4510U N7510	N8800PRO N12000V N16000V N7700PRO V2 N8800PRO V2 N10850 N8850	N8900 N12000 N16000
Allowed iSCSI volume	15	25	50

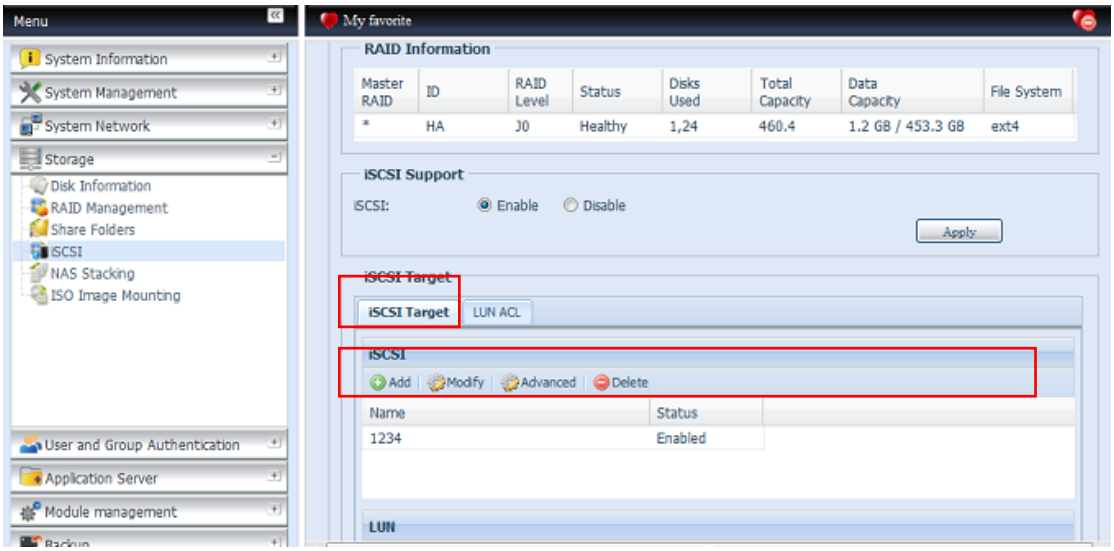


iSCSI Target

To add iSCSI target volume, click **iSCSI** with associated RAID volume from its drop down list and select the desired RAID volume.

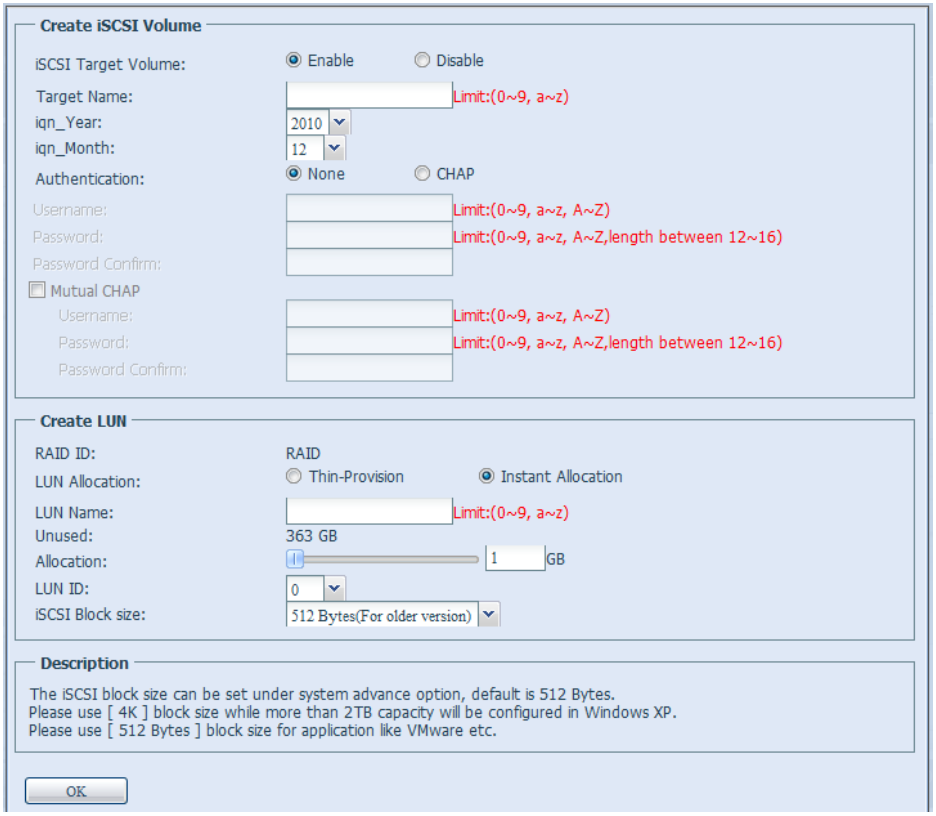
iSCSI Target	
Item	**Description**
Add	Click to allocate space to iSCSI target from associated RAID volume.
Modify	Click this to modify the iSCSI Target.
Advanced	There are 3 options (iSCSI CRC/Checksum, Max Connections, Error Recovery Level) These currently allow the Admin to Enable/Disable the Thecus IP storage associated with the iSCSI setting.
Delete	Click this to delete the iSCSI Target.

Allocating Space for iSCSI Volume



To allocate space for an iSCSI target on the current RAID volume, follow the steps below:

1. Under the **iSCSI Target List**, select ***iSCSI Target then click Add***. The **Create iSCSI Volume** screen appears.



Create iSCSI Volume	
Item	**Description**
iSCSI Target Volume	Enable or Disable the iSCSI Target Volume.
Target Name	Name of the iSCSI Target. This name will be used by the **Stackable NAS** function to identify this export share.
iqn_Year	Select the current year from the dropdown.

Iqn_Month	Select the current month from the dropdown.
Authentication	You may choose CHAP authentication or choose None.
Username	Enter a username.
Password	Enter a password.
Password Confirm	Reenter the chosen password
Mutual CHAP	With this level of security, the target and the initiator authenticate each other.
Username	Enter a username.
Password	Enter a password.
Password Confirm	Reenter the chosen password
RAID ID	ID of current RAID volume.
LUN Allocation	Two modes can be choose from: Thin-provision：iSCSI thin-provisioning shares the available physical capacity to multiple iSCSI target volumes. It allows virtual capacity to be assigned to targets prior to adding physical space when it has run out. Instant Allocation: Allocate available physical capacity to iSCSI target volumes.
LUN Name	Name of the LUN.
Unused	Unused space on current RAID volume.
Allocation	Percentage and amount of space allocated to iSCSI volume.
LUN ID	Specific Logic unit ID number.
iSCSI Block size	The iSCSI block size can be set under system advance option, default is 512 Bytes. [4K] block size while more than 2TB capacity will be configured in Windows XP. [512 Bytes] block size for application like VMware etc.

NOTE Be sure the iSCSI target volume has been enabled or it will not list out while using Initiator to get associated iSCSI target volumes.

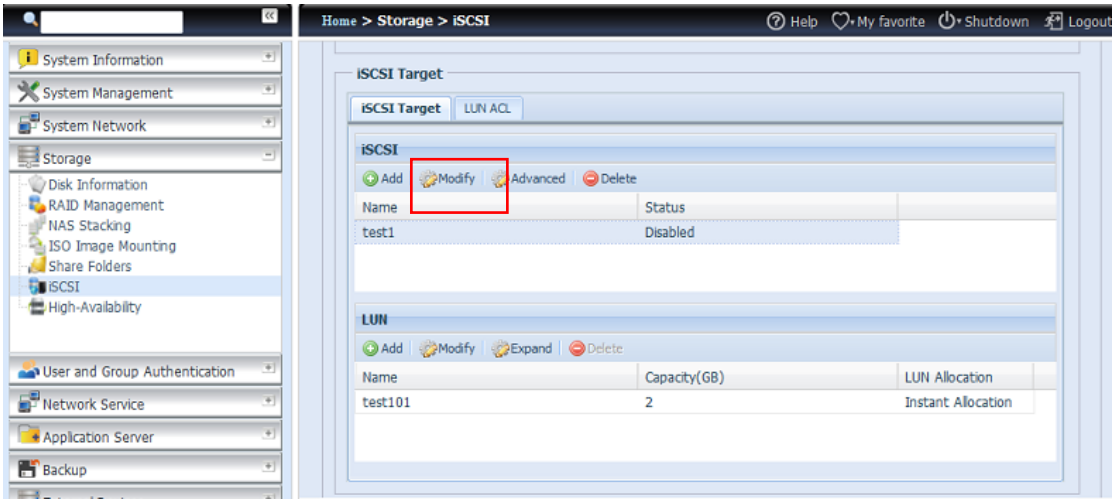
NOTE The iSCSI target volume creation will associate at least one LUN together. It can be assigned either "Thin-Provisioning" or "Instant Allocation".

2. Enable the **iSCSI Target Volume** by selecting ***Enable***.
3. Enter a **Target Name**. This will be used by the **Stackable NAS** function to identify this export share.
4. Choose the current year from the **Year** dropdown.
5. Choose the current month from the **Month** dropdown.
6. Choose to enable ***CHAP*** authentication or choose ***None***.
7. If you've enabled CHAP authentication, enter a **username** and a **password**. Confirm your chosen password be reentering it in the **Password Confirm** box.
8. Choose **Thin-Provision** or **Instant Allocation**
9. Enter a **LUN Name**.
10. Designate the percentage to be allocated from the **Allocation** drag bar.
11. When iSCSI target volume has been created, the LUN ID is configurable from 0 to 254 with a default of the next available number in ascending numerical order. The LUN ID is unique and cannot be duplicated.
12. Choose **[4K] block size** to have iSCSI target volume over 2TB barrier or **[512 Bytes] block size** in some application needed.
13. Click ***OK*** to create the iSCSI volume.

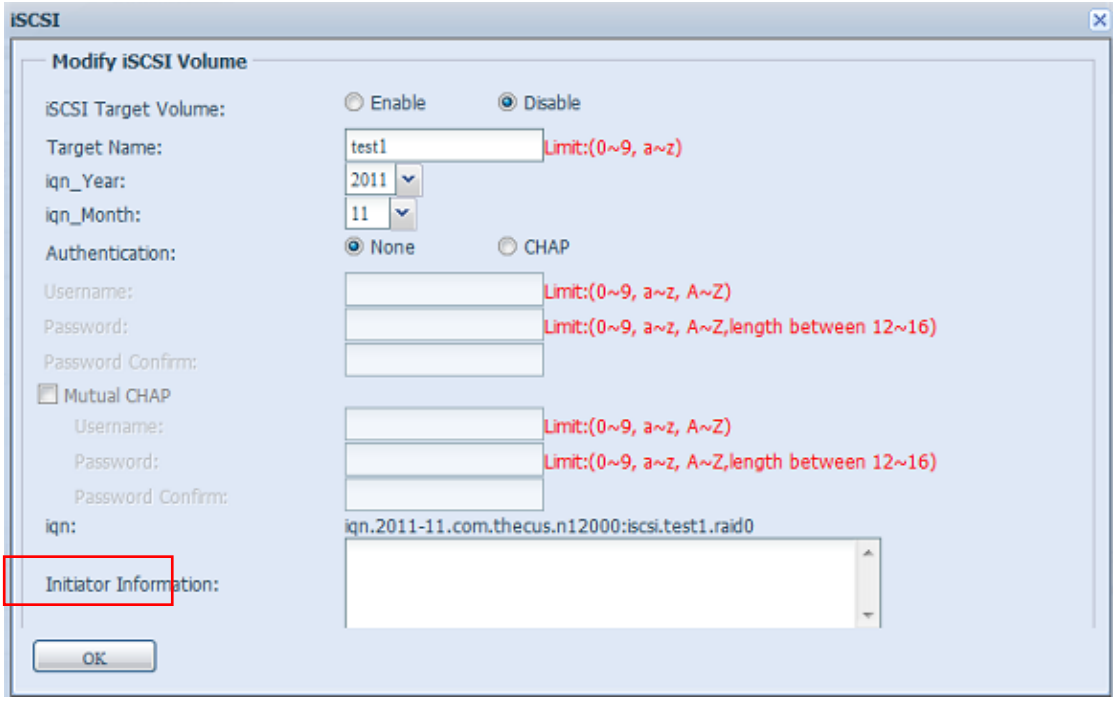
Modify iSCSI Volume

To modify iSCSI target on the current RAID volume, follow the steps below:

1. Under the **iSCSI Target List**, click ***Modify***.
   The **Modify iSCSI Volume** screen appears.

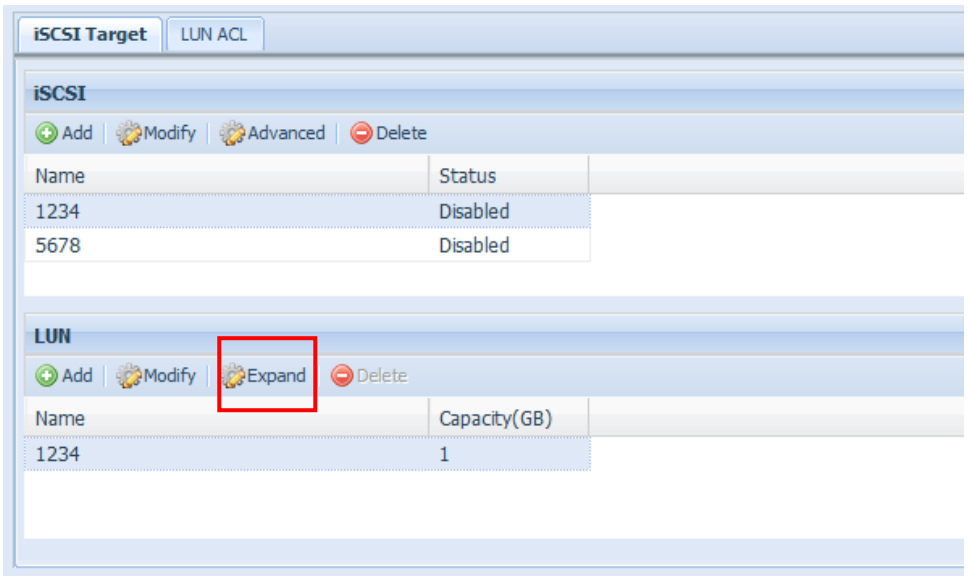


2. Modify your settings. Press **ok** to change.

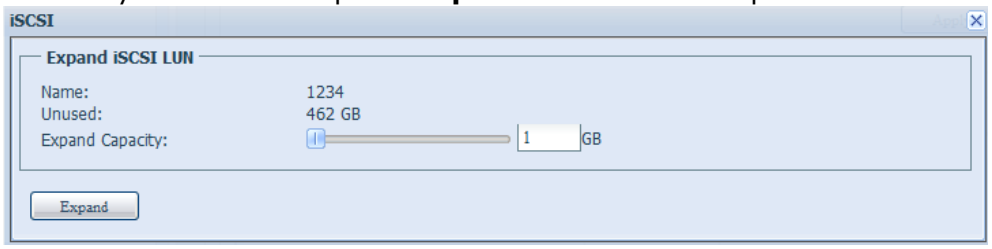


Expand Volume

The iSCSI volume is now able to expand its capacity from unused space (Instant Allocation mode only). From the volume list, simply select the iSCSI volume you like to expand and click the **Expand** button:



You will then see the dialog box displayed below. Drag the **Expand Capacity** bar to the size you want. Then press **Expand** to confirm the operation.



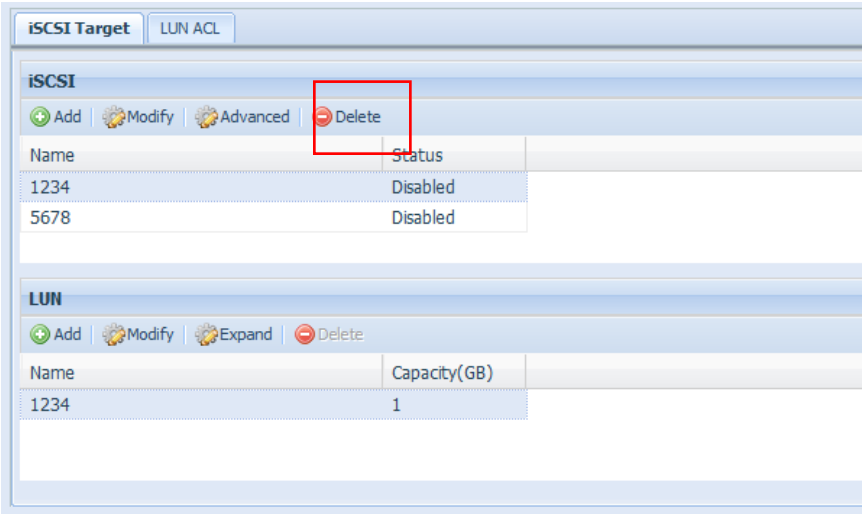
NOTE

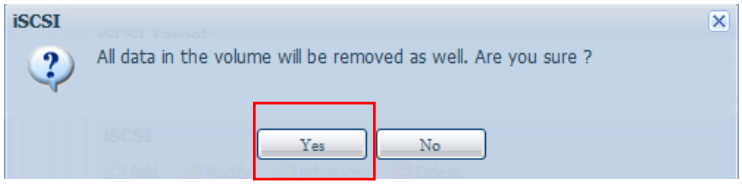
The iSCSI expand is only capable while iSCSI target volume is crested by "Instant Allocation". iSCSI target created by "Thin Provisioning" has virtual space assigned during the initial stage, so it has no expandable capability.

Delete Volume

To delete volume on the current RAID volume, follow the steps below:

1. Under the **Volume Allocation List**, click ***Delete***.
   The **Space Allocation** screen appears.



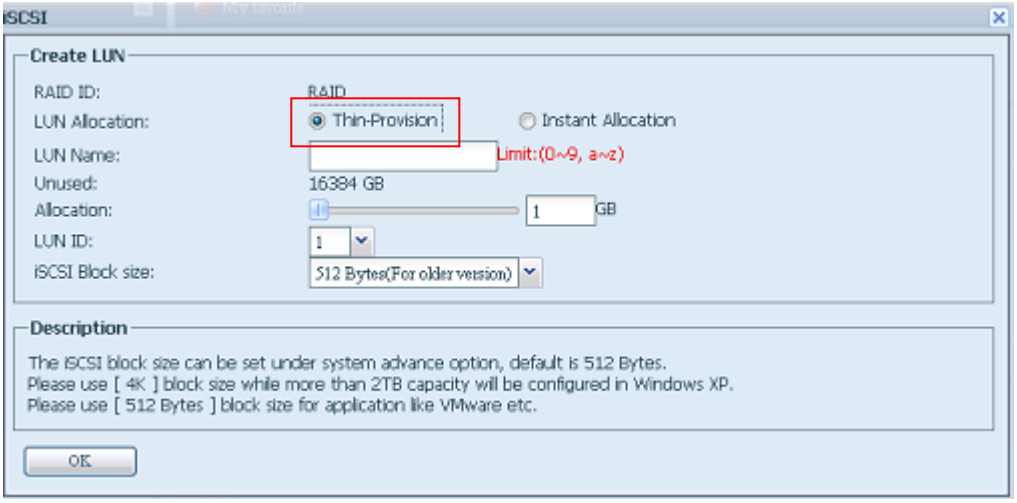


2. Press **YES**. All data in the volume will be removed.

iSCSI Thin-Provisioning

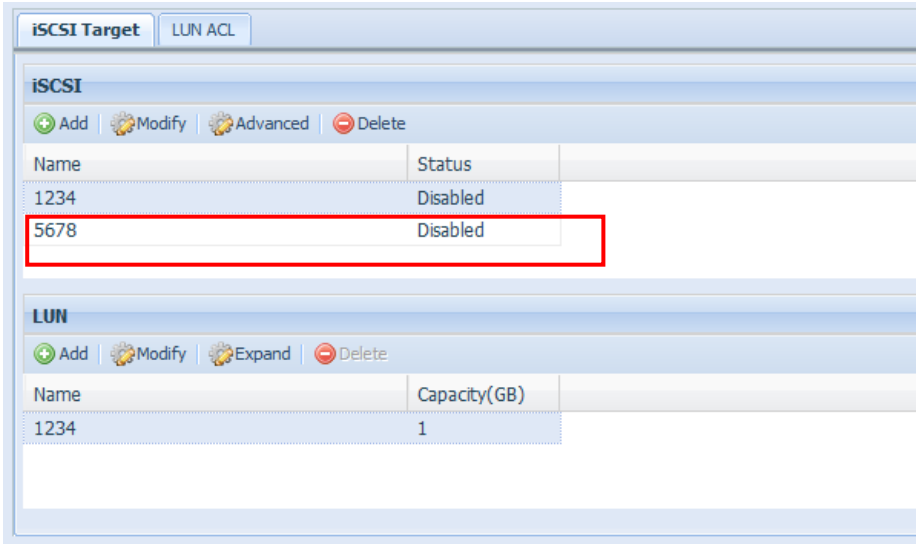
If iSCSI Thin-Provisioning is selected when creating an iSCSI target volume, virtual memory is assigned to the target, allowing the physical memory to reach maximum capacity and adding new disks only when needed.

To setup iSCSI thin-provisioning, simply select "Thin-Provision" mode from the "Create LUN" setting screen.



Next, allocate capacity for the iSCSI thin-provision volume by dragging the **Allocation** bar to the desired size.

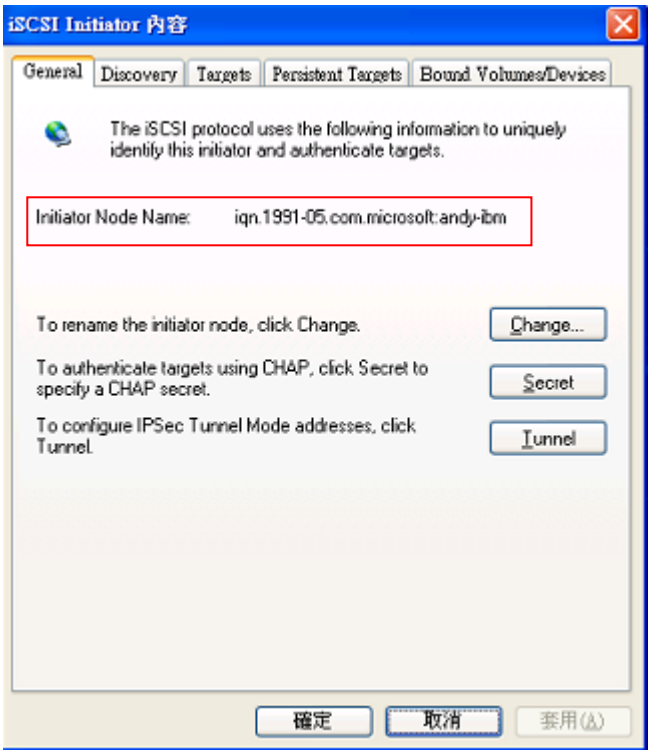
After the size has been determined, click **OK** to confirm. Now you will see the iSCSI thin-provisioning volume is available from the list. Please refer to the screenshot below.



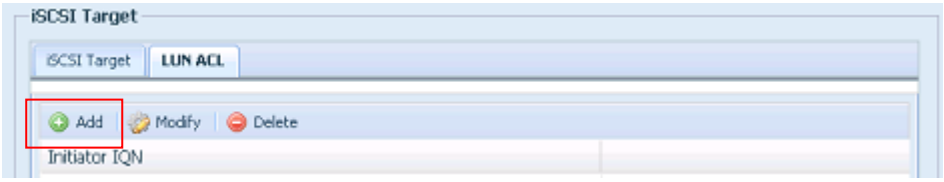
If creating an iSCSI target volume under "Instant Allocation", physical memory is assign to the target, being limited by the available memory. For the iSCSI target volume created under "thin-provisioning", virtual memory is assigned to the volume, which can go up to 16384GB (16TB).

LUN ACL

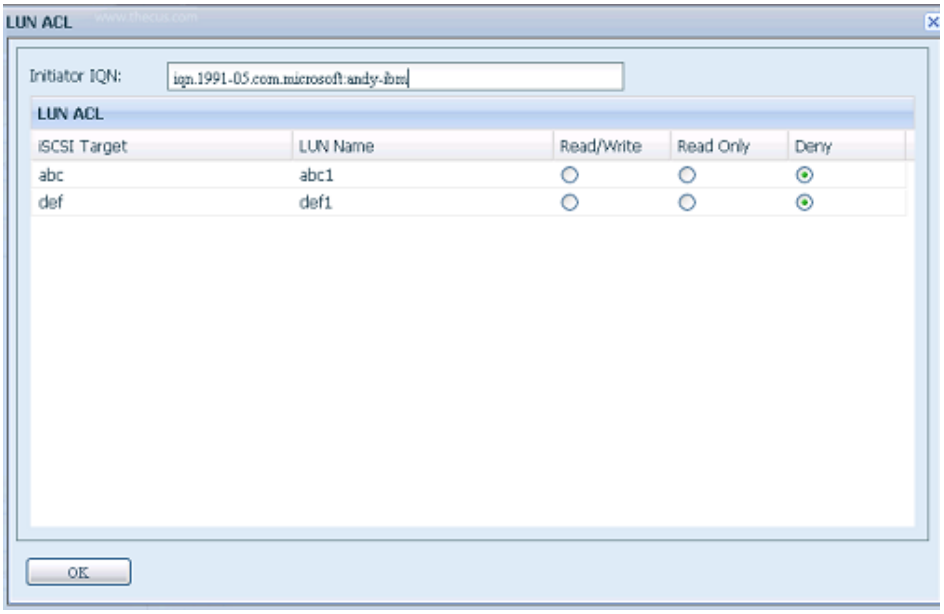
After iSCSI target has been created, you are one step away from using the iSCSI volume. Under "LUN ACL", you need to add "Initiator iqn" and setup ACL access privileges to determine the accessibility. Please refer the screen shot below for where "Initiator iqn" can be found.



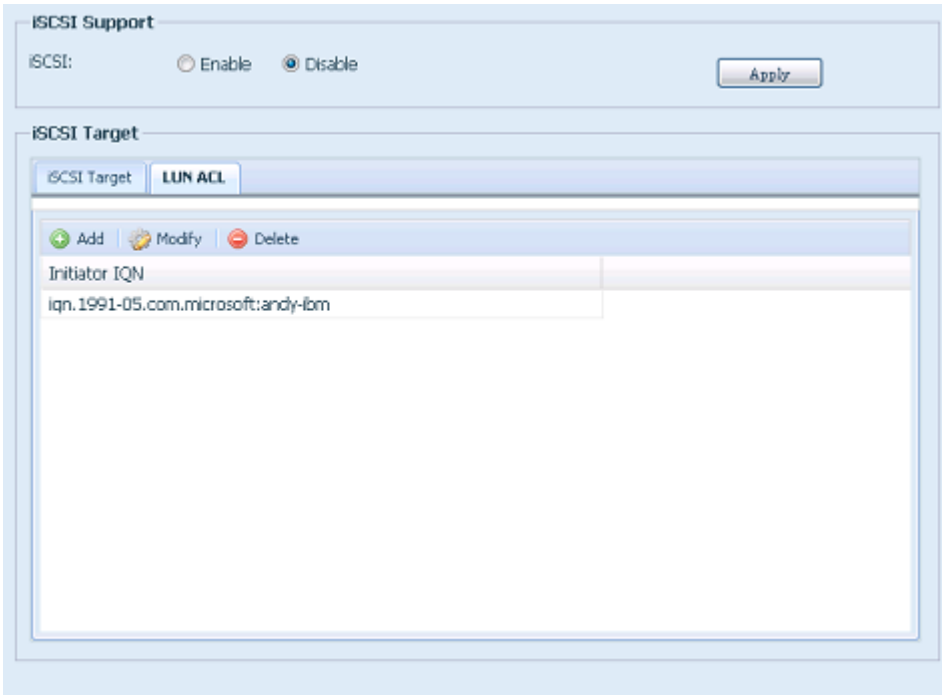
From the LUN ACL setting screen click "Add":



Next, input "Initiator iqn" and setup iSCSI target volume access privileges from the available list. Apply by clicking the OK button.



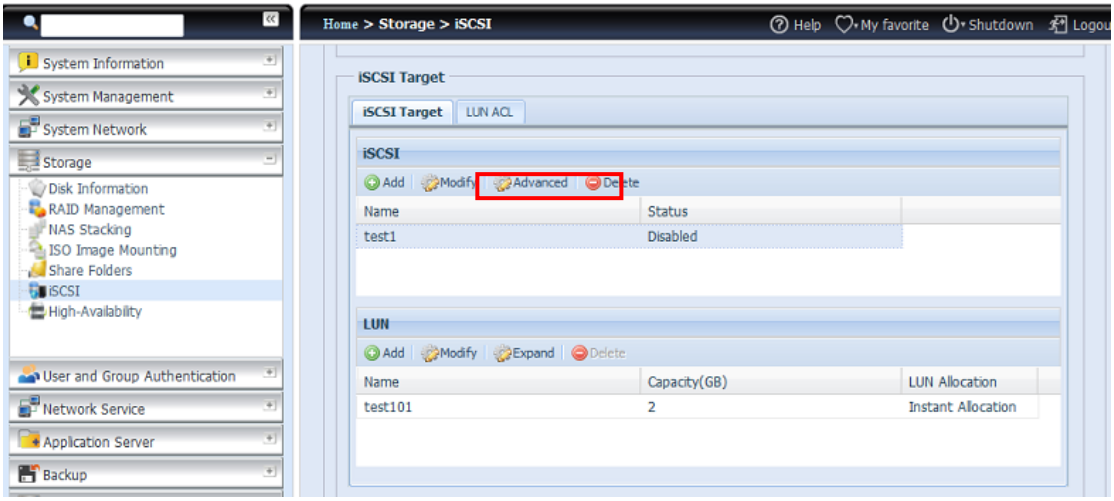
The accessible Initiator will be listed as shown in the screen shot displayed below.



The listed "Initiator iqn" can be modified or deleted by selecting the desired iqn and pressing Modify or Delete.

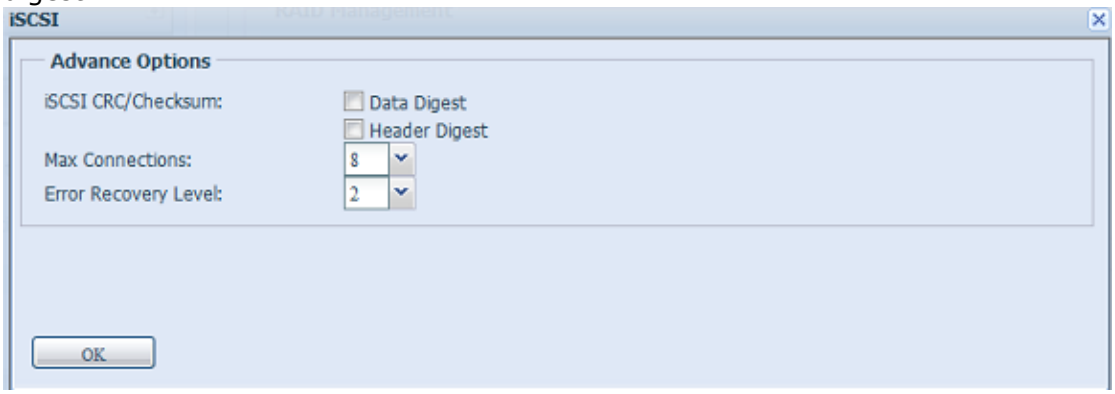
Advance Option

There are 3 available options for the user to operate Thecus IP storage associated with iSCSI setting. The details are listed in the following screenshot. If the options are modified, the system will need to reboot for the changes to take place.



iSCSI CRC/Checksum

To enable this option, the initiator can connect with "Data digest" and "Header digest".



Max Connections

The maximum number of iSCSI connections.

Error Recovery Level

The Error Recovery Level (ERL) is negotiated during a leading iSCSI connection login in traditional iSCSI (RFC 3720) and iSER (RFC 5046).

ERL=0: Session Recovery

ERL=0 (Session Recovery) is triggered when failures within a command, within a connection, and/or within TCP occur. This causes all of the previous connections from the failed session to be restarted on a new session by sending a iSCSI Login Request with a zero TSIHRestart all iSCSI connections on any failure.

ERL=1: Digest Failure Recovery

ERL=1, only applies to traditional iSCSI. For iSCSI/SCTP (which has its own CRC32C) and both types of iSER (so far), handling header and data checksum recovery can be disabled.

ERL=2: Connection Recovery

ERL=2, allows for both single and multiple communication path sessions within a iSCSI Nexus (and hence the SCSI Nexus) to actively perform realligence/retry on iSCSI ITTs from failed iSCSI connections. ERL=2 allows iSCSI fabrics to take advantage of recovery in all regards of transport level

fabric failures, and in a completely OS independent fashion (i.e. below the host OS storage stack).

High-Availability (N8900, N12000 series/N16000 series only)

HA keeps your data active on two separate systems, Thecus Supports Active/Passive HA — provides a fully redundant instance of each node, which is only brought online when its associated primary node fails.

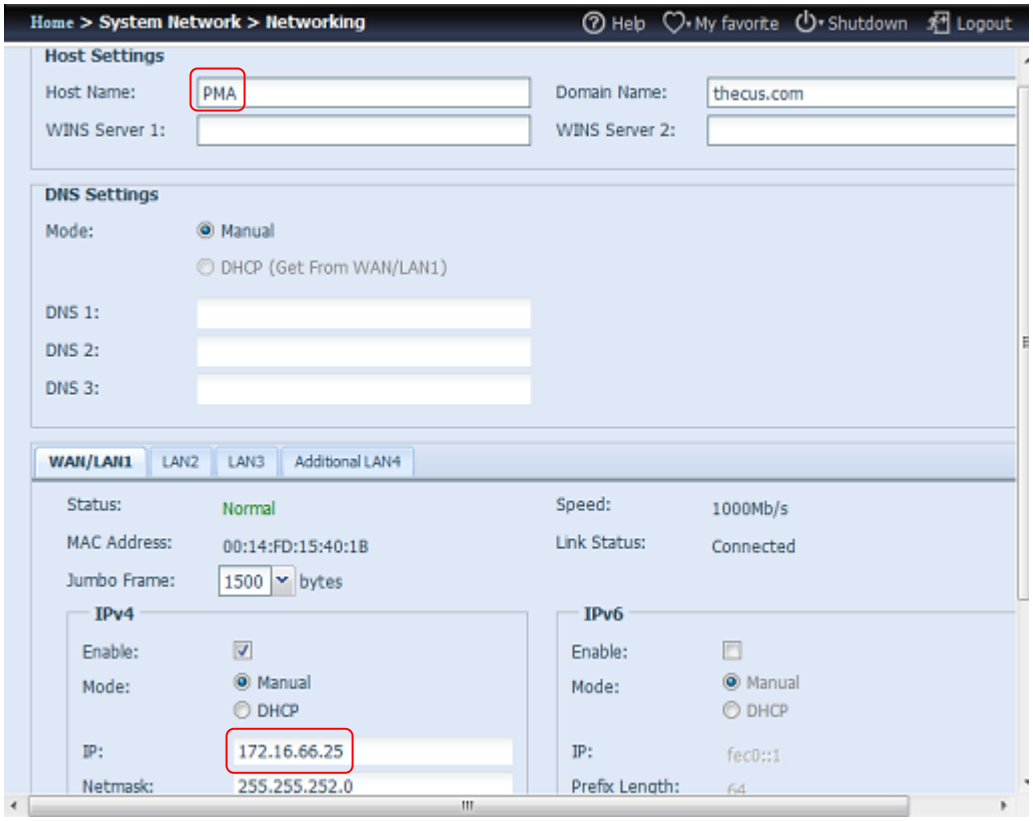
HA setup procedure:

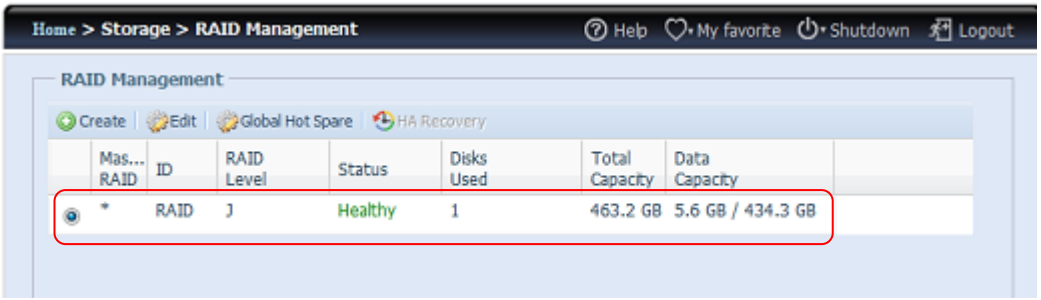
HA needs two **identical** Thecus systems (same models and same hard disk slot installed) which are capable for high availability features. One needs to be setup as "Primary" and the second unit as "Secondary", both units' needs to have the RAID volume build up prior installation.

WARNING

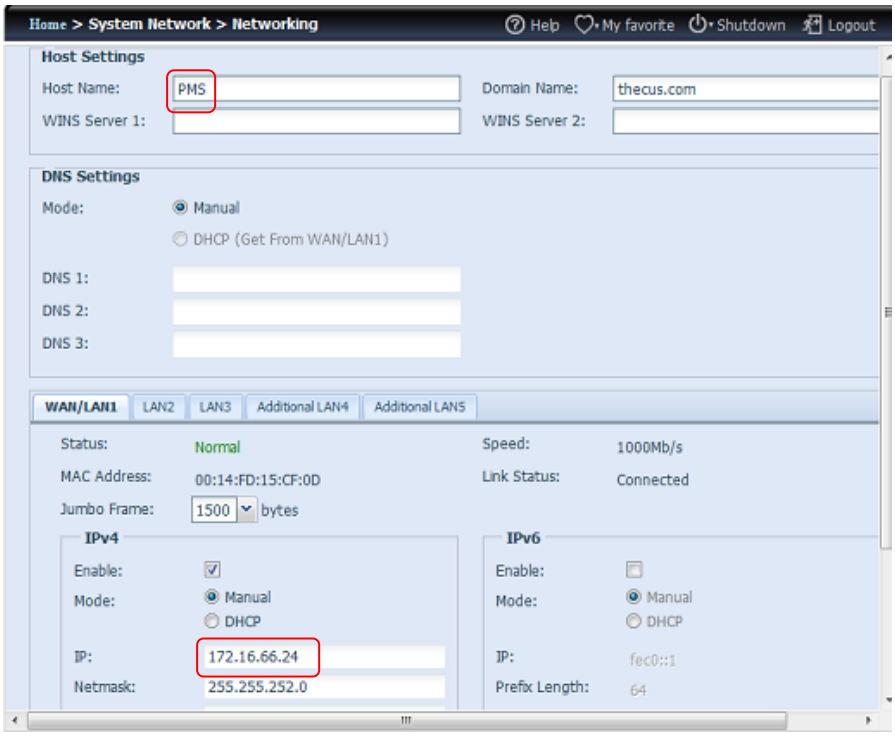
Please be notified that if the system has been used as a standalone station before and contained more than one RAID volume with data inside, once it is used for HA, all of data will be destroyed.

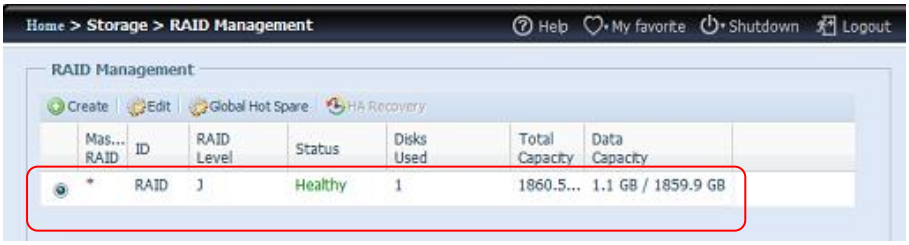
Let's see an example with two Thecus Units.
1st unit: Host name: PMA (172.16.66.25) with JBOD RAID volume. This unit will be setup as the Primary server.





2nd unit: Host name: PMS (172.16.66.24) with JBOD RAID volume. This unit will be setup as the Secondary server.



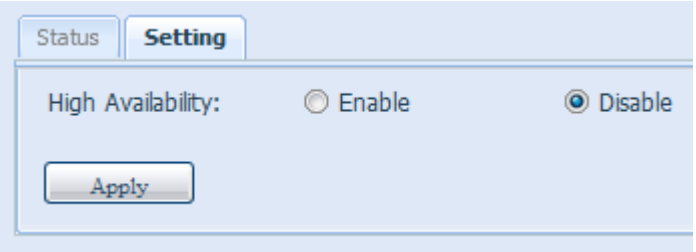


WARNING **The HDD capacity of HA Secondary server must be equal or greater than the Primary server or a warning message will appear.**

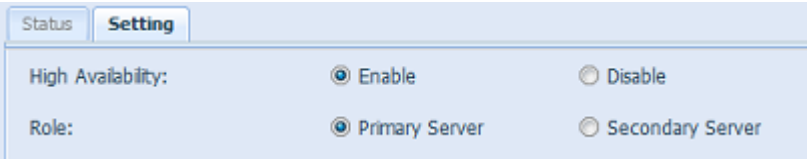
Setting up the Primary unit for HA. Let's use the Primary unit from our example PMA (172.16.66.25):

i. Login in to web UI of system 172.16.66.25. Then go to "High Availability" HA configuration page under the Storage category.

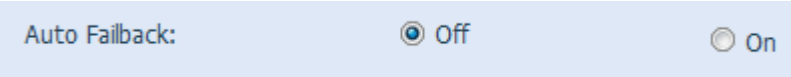
ii. Click on "Enable" radio button, then the setting page will appear.



iii. Choose the server role of the system, for this example, we will have this unit as 'Primary Server". So "Primary Server" is checked.

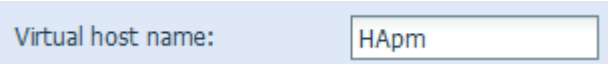


iv. Choose the "Auto Failback" option, the default is disabled. For more details about auto failback, please refer to the description below.

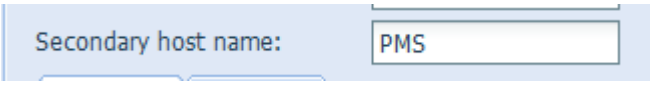


Auto Fail Back:	In legacy Heartbeat clusters, the auto failback option would determine whether a resource would automatically fail back to its "Active" node, or remain on whatever node is serving it until that node fails, or an administrator intervenes. The possible values for auto failback were: on - enable automatic failbacks off - disable automatic failback When auto failback is off (default): After the original active server is damaged and then returned to a healthy state, the original standby server will remain active and the original active server will go into standby mode. The servers will exchange roles. When auto failback is on: After the original active server is damaged and then returned to a healthy state, the original standby server will go back into standby mode and the original active server will become active again. The servers return to their original roles. With or without auto failback, synchronization will begin immediately without a break in service when the damaged server returns. The roles described above are assumed immediately and do not need to wait for synchronization. The virtual IP will always be mapped to the current active server.

v. Fill in the "Virtual Server" hostname information for further access need. For this example, we will use "HApm" for the virtual server hostname.

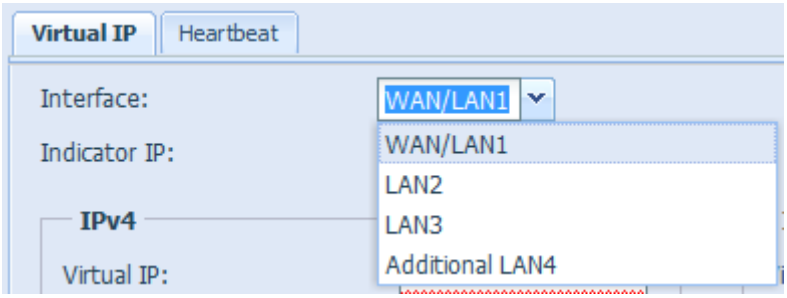


vi. Fill in the "Secondary Server" hostname information. For this example, we will use "PMS" for the secondary server hostname. Please make sure the associated Secondary server with the "PMS" host name has been setup.

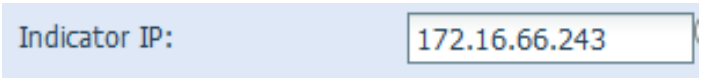


vii. Fill in the "Virtual IP" information:

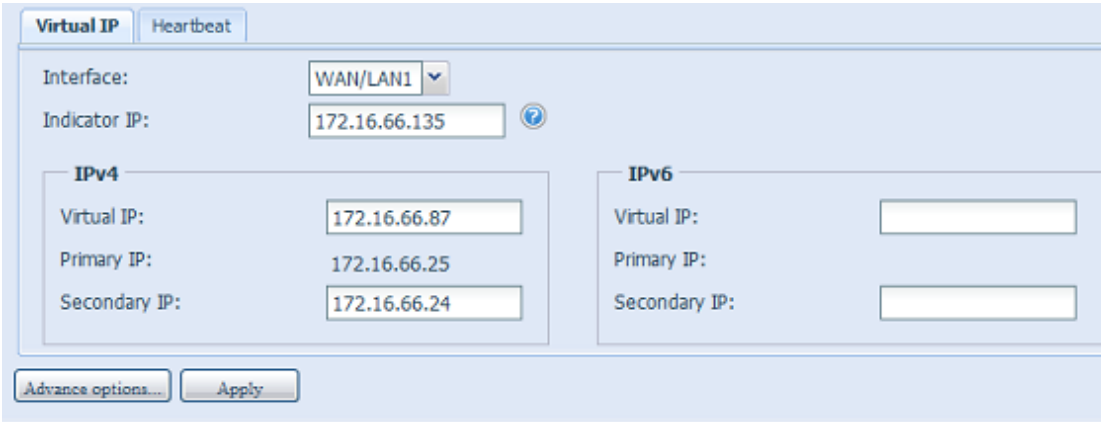
1. Please select the network interface from the drop down list of physical connective available. It can be either on board LAN ports or additional add-in NIC, even 10G.



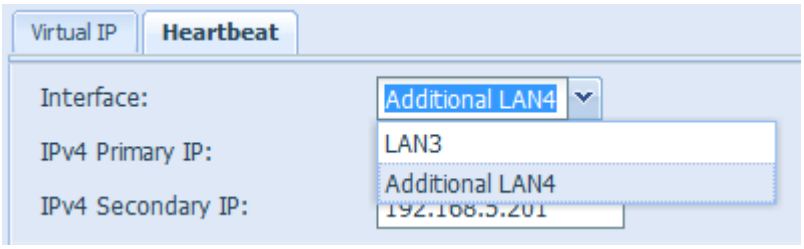
2. Input "Indicate" IP address. This "indicate IP" is used for the system to ping out then check whether the system is still alive. So please input an IP address that is going to response properly.

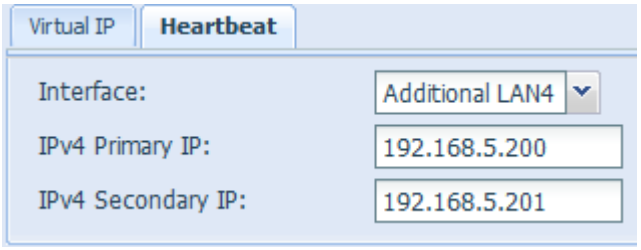


3. Filled in IP information for the "Virtual IP" and "Secondary Server IP" in either IPv4 or IPv6. For our example we chose the "WAN/LAN1" for the connection interface and virtual IP 172.16.66.87. The secondary server IP address is 172.16.66.24 has mentioned earlier.

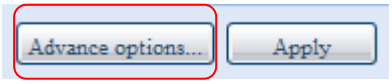


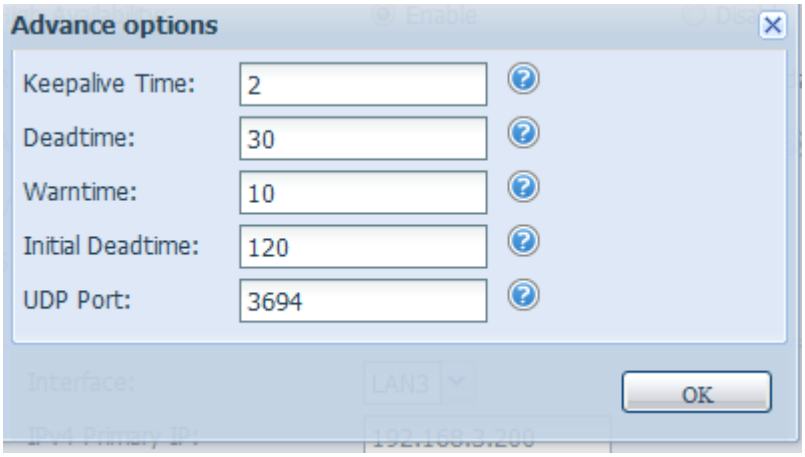
viii. Choose the network interface for heartbeat in between the systems. It can be selected from the drop down list, if there is additional LAN card that has been installed, such as 10G card, it can be used for the heartbeat role. After inserting the IP addresses for direct link needed in between the primary and secondary servers, default value will appear. Normally, no modifications will be required.
The example here we will use the "Additional LAN4" which is a 10G NIC to be used for the heartbeat link between the primary and secondary servers.





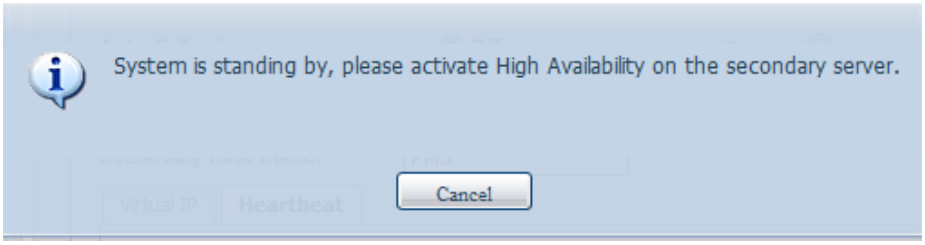
ix. Advance options can be setup by pressing the associated button.





Heart Beats Configuration	
Item	**Description**
Keep alive time	The keep alive directive sets the interval between heartbeat packets. It is specified according to the Heartbeat time syntax.
Dead time	The dead ping directive is used to specify how quickly Heartbeat should decide that a ping node in a cluster is dead. Setting this value too low will cause the system to falsely declare the ping node dead. Setting it too high will delay detection of communication failure. This feature has been replaced by the more flexible ping resource agent in Pacemaker, and should no longer be used.
Warning time	The warn time directive is used to specify how quickly Heartbeat should issue a "late heartbeat" warning.
Initial dead time	The initial dead parameter is used to set the time that it takes to declare a cluster node dead when Heartbeat is first started. This parameter generally needs to be set to a higher value, because experience suggests that it sometimes takes operating systems many seconds for their communication systems before they operate correctly.
UDP port	The udp port directive specifies which port Heartbeat will use for its UDP intra-cluster communication. The default value for this parameter is UDP 694 port.

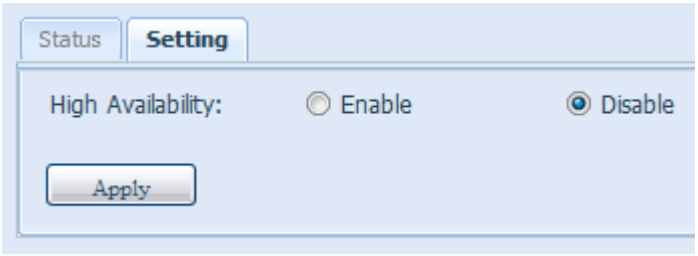
x. Click "Apply", the Primary server will prompt the message below and wait for the "Standby" server settings to be completed.



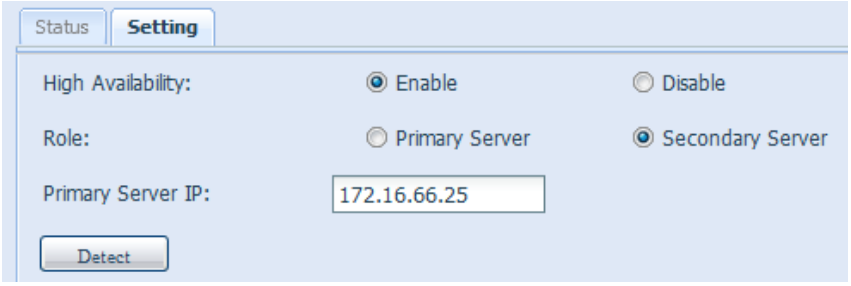
Setting up the Secondary unit for HA. The secondary unit for our example is PMS (172.16.66.24):

xi. Login in to the web UI of the system 172.16.66.24 then go to "High Availability" HA configuration page under the Storage category.

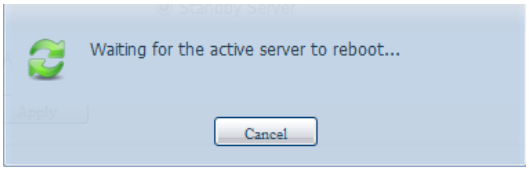
xii. Click on the "Enable" radio button, the setting page will appear.



xiii. Choose the server role of the system, for this example, we will have this unit set as the "Secondary Server". So "Secondary Server" is checked. After, please fill in the associated "Primary Server" IP address.

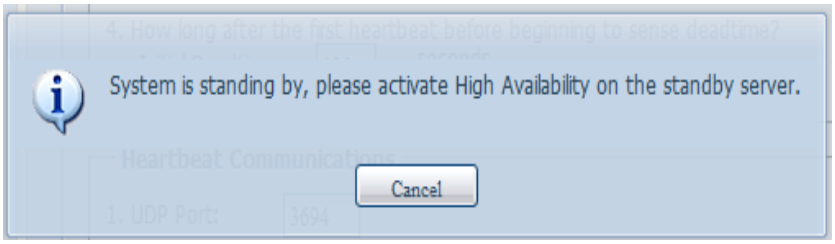


xiv. Click "Detect" and the Secondary unit will start to check for the Primary server status. If the Primary server has replied properly, then the message will appear as below.

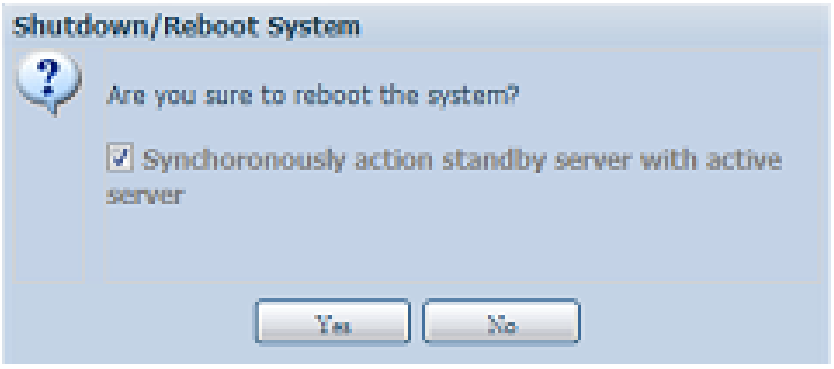


Please check the Primary Server unit. You will see an interactive message saying to reboot both "Primary" and 'Secondary" server together to complete the High Availability settings.

The last state of the Primary server is: waiting for the Secondary server as shown in the screen shot below:

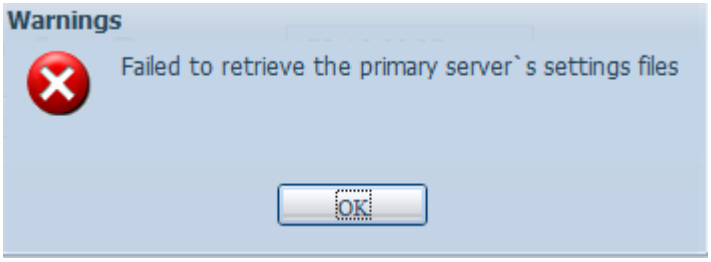


After the Secondary server has communicated with Primary Server successfully, then the state will changed to:



Click "Yes" to reboot both Primary and Secondary server.

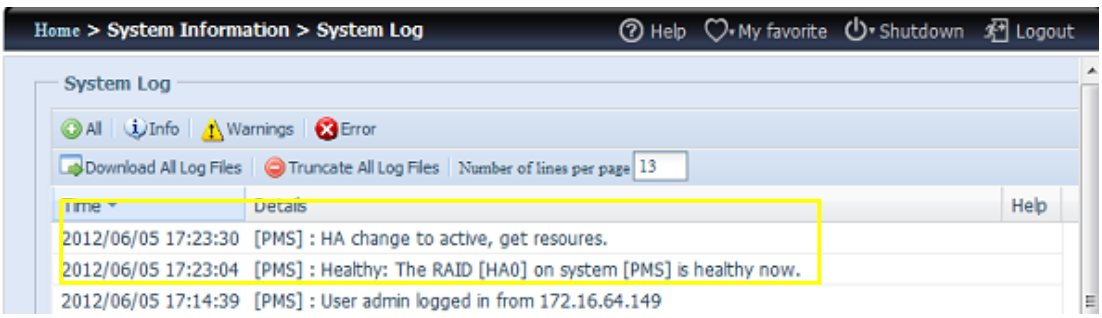
If the communication has failed then you will see an error message as below.



Conditions in which the secondary server will take over to play the role as Active:

1. Primary server RAID is damaged
2. Loss of the primary server's data port connection
3. Primary server goes down for any other reason

When the primary server encounters the above-mentioned situations, the secondary server (PMS) will immediately take over to play the role as active. The secondary server's system log will show "HA changed to active, getting resources", and "Healthy: The RAID [HA] on system [PMS] is healthy now."

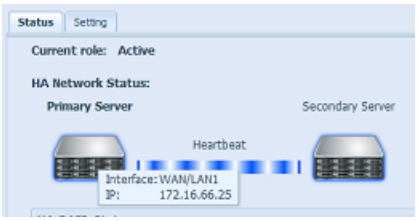


At this time, the virtual IP address will be mapped to the PMS system because it is in an active state.

HA Ready:

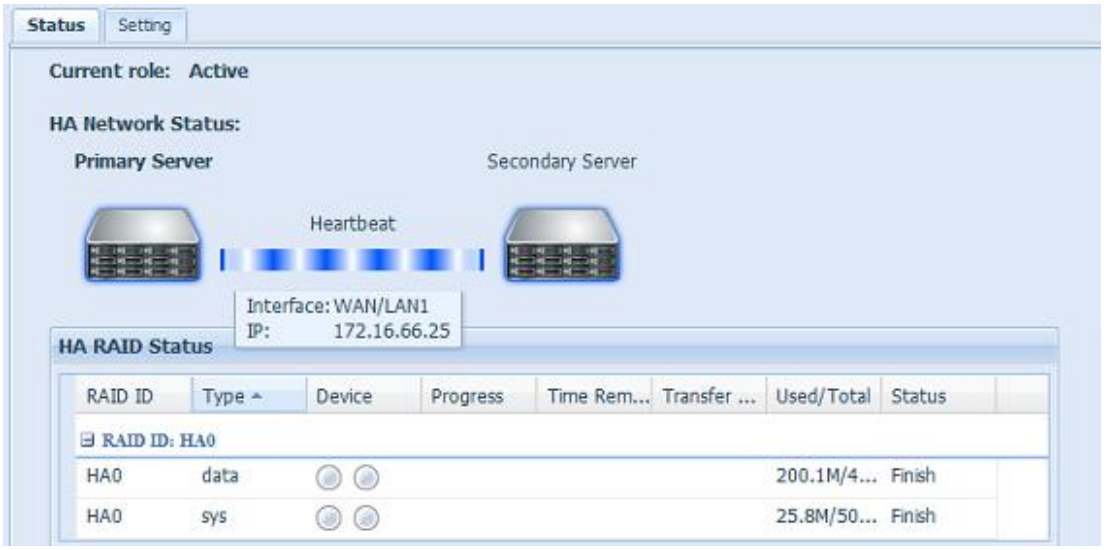
After both Primary and Secondary systems has rebooted, the HA link status and the HA RAID volume can be seen from the HA status page.

Please note, it will take 1~2 minutes to complete the primary and secondary servers' role played. If both servers are displayed as standby, please wait for the systems to synchronize with each other.

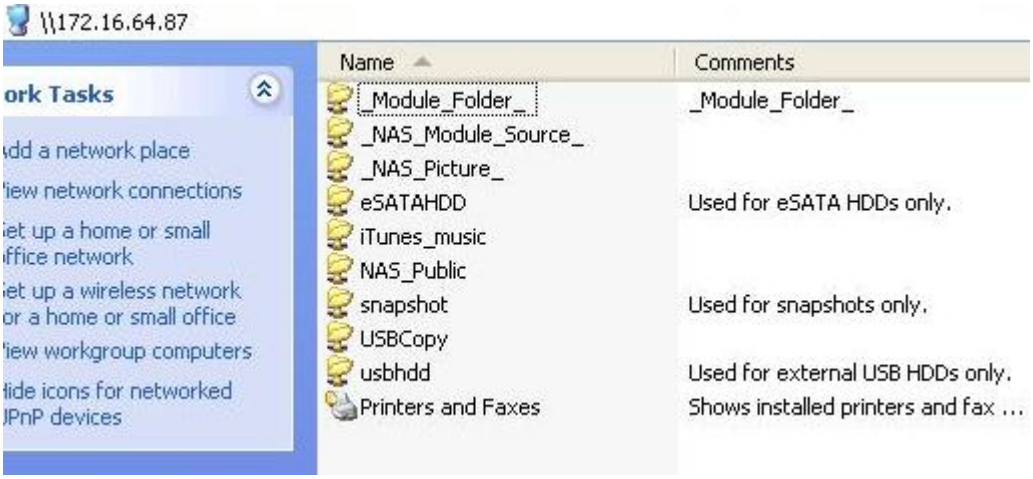


From the HA Primary server "PMA (172.16.66.25)" it will denote the role of "Active" and for the "PMS (172.16.66.24)", it will show the role as Standby.

The HA RAID volume status can be found as shown in the screen shot below.

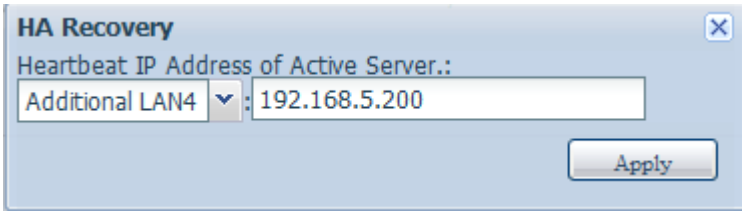


The user can access this newly create HA system by its virtual IP. Using widows, the user can simply input 172.16.64.87 or HApm in the navigation bar then the available share files will be listed as below:

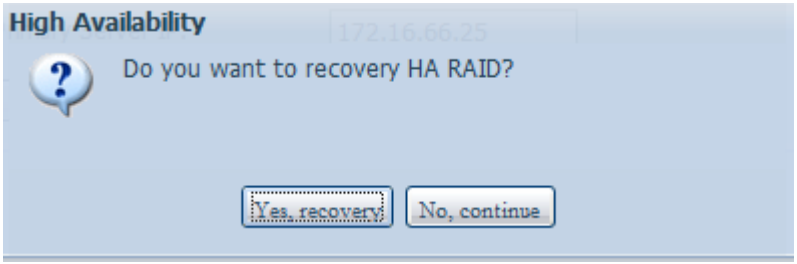


HA Recovery:

If one of the HA member is down and need to be recovered, simply go to the RAID management page and the "HA Recovery" icon will be available.
Click on the "HA Recovery" icon, then the system will prompt a box to inquire about the Active server heartbeat link IP address. After inputting the IP address and pressing Apply, the unit will be recovered fully.



Another circumstance where HA recovery might be needed is when the HA button has been enable but the system detected a previously existing HA configuration. Then the screen will prompt the message box as shown below:



If the other HA member is running smoothly, please choose "Recovery HA" to complete HA recovery. Or select "No, continue" to let both HA members has they are.

WARNING

If there are transfers in progress when the Primary server encounters problems and the Secondary server becomes active, the session will be stopped. Please contact your network administrator to determine whether or not your transfers were completed.

WARNING

When the original primary server rejoins the HA environment, it will be updated with the newer data from the secondary server to synchronize for HA. Please be aware that the data on the original primary server will be replaced by the data from the secondary server.

User and Group Authentication

The Thecus IP storage has built-in user database that allows administrators to manage user access using different group policies. From the **User and Group Authentication** menu, you can create, modify, and delete users, and assign them to groups that you designate.

ADS/NT Support

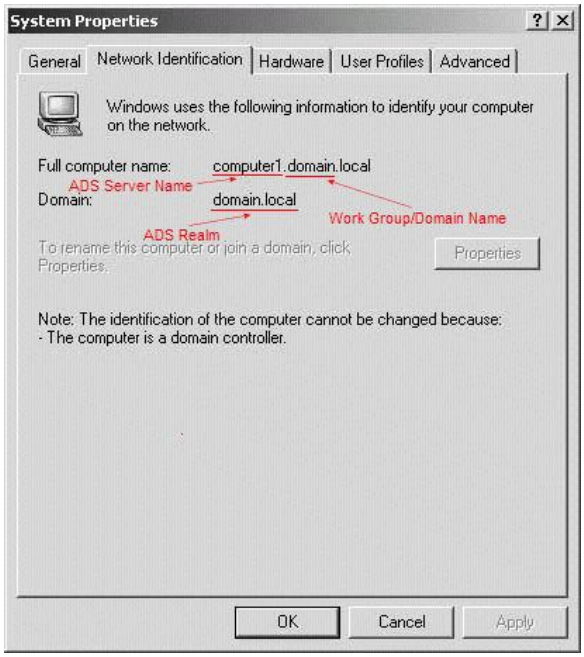
If you have a Windows Active Directory Server (ADS) or Windows NT server to handle the domain security in your network, you can simply enable the ADS/NT support feature; the Thecus IP storage will connect with the ADS/NT server and get all the information of the domain users and groups automatically. From the **Accounts** menu, choose ***Authentication*** item and the **ADS/NT Support** screen appears. You can change any of these items and press ***Apply*** to confirm your settings.

A description of each item follows:

ADS/NT Support

Item	Description
Work Group / Domain Name	Specifies the SMB/CIFS Work Group / ADS Domain Name (e.g. MYGROUP).
ADS Support	Select Disable to disable authentication through Windows Active Directory Server.
ADS Server Name	Specifies the ADS server name (e.g. adservername).
ADS Realm	Specifies the ADS realm (e.g. example.com).
Administrator ID	Enter the administrators ID of Windows Active Directory, which is required for Thecus IP storage to join domain.
Administrator Password	Enter the ADS Administrator password.
Apply	To save your settings.

To join an AD domain, you can refer to the figure here and use the example below to configure the Thecus IP storage for associated filed input:



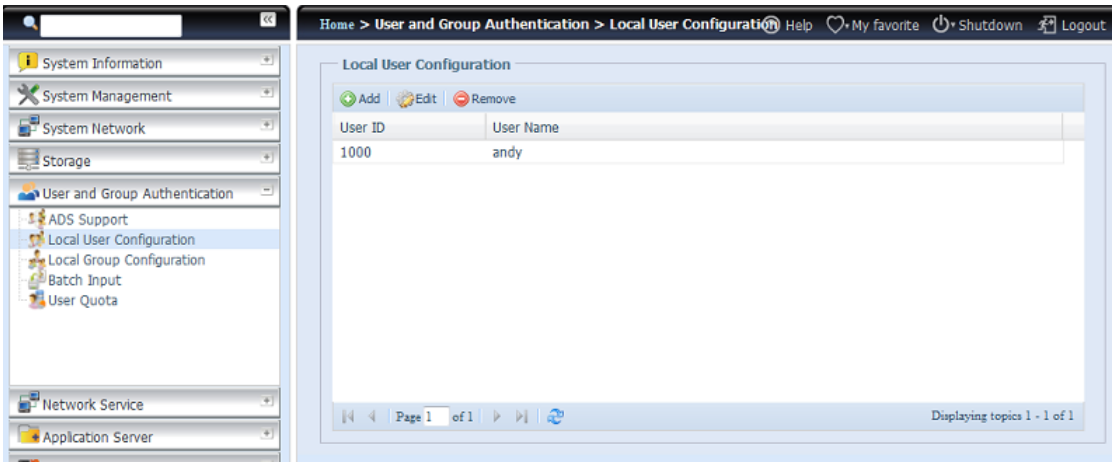
AD Domain Example	
Item	**Information**
Work Group / Domain Name	domain
ADS Support	Enable
ADS Server Name	Computer1
ADS Realm	Domain.local
Administrator ID	Administrator
Administrator Password	**********

NOTE

- The DNS server specified in the WAN/LAN1 configuration page should be able to correctly resolve the ADS server name.
- The time zone setting between Thecus IP storage and ADS should be identical.
- The system time difference between Thecus IP storage and ADS should be less than five minutes.
- The Administrator Password field is for the password of ADS (Active Directory Server) not Thecus IP storage.

Local User Configuration

From the **Accounts** menu, choose the **User** item, and the **Local User Configuration** screen appears. This screen allows you to **Add**, **Edit**, and **Remove** local users.



Local User Configuration	
Item	**Description**
Add	Press the ***Add*** button to add a user to the list of local users.
Edit	Press the ***Edit*** button to modify a local user.
Remove	Press the ***Remove*** button to delete a selected user from the system.

Add Users

1. Click on the ***Add*** button on **Local User Configuration** screen, and **Local User Setting** screen appears.

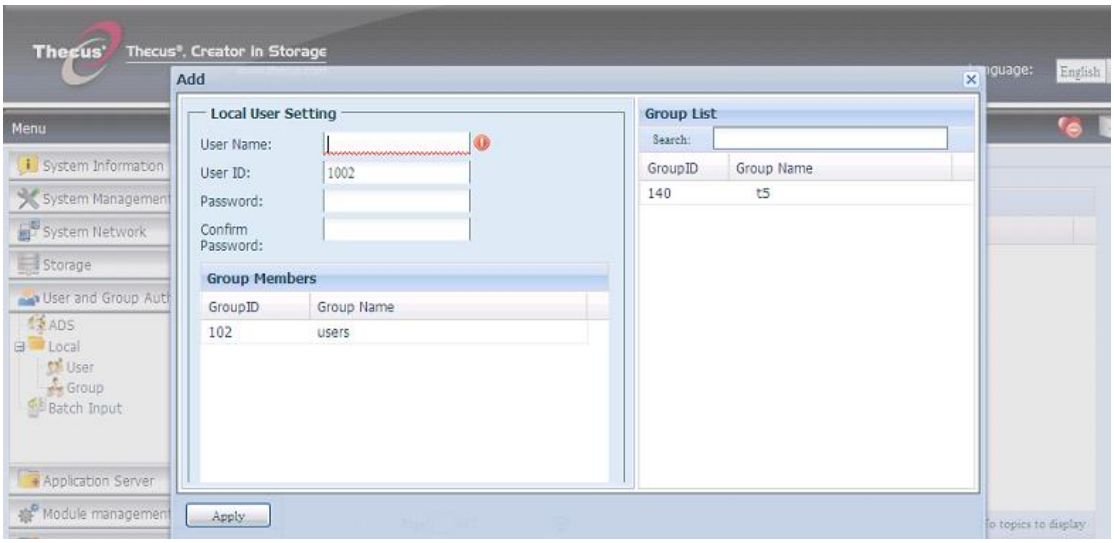
2. On the **Local User Setting** screen, enter a name in the **User Name** box.

3. Enter a **User ID** number or leave blank to use the system default value.

4. Enter a password in the **Password** box and re-enter the password in the **Confirm** box.

5. Select which group the user will belong to. **Group Members** is a list of groups this user belongs to. **Group List** is a list of groups this user does not belong to. Use the **<<** or **>>** buttons to have this user join or leave a group.

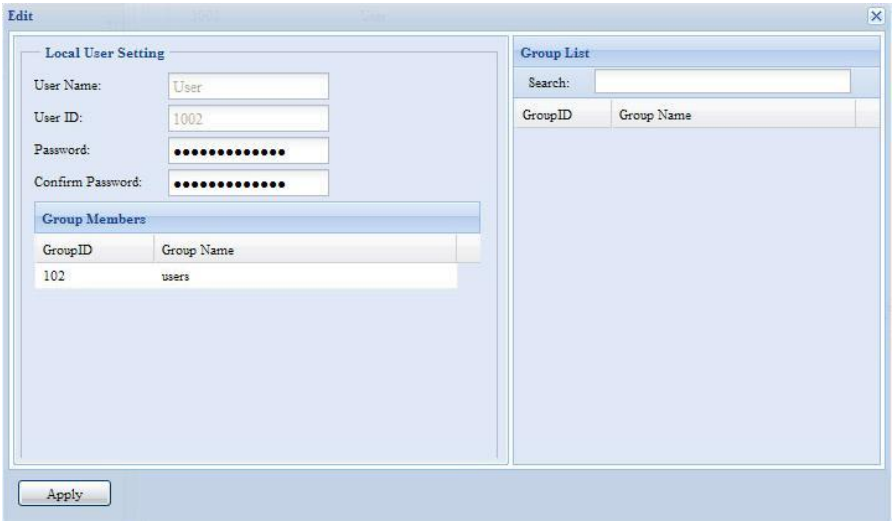
6. Press the ***Apply*** button and the user is created.



NOTE All users are automatically assigned to the 'users' group.

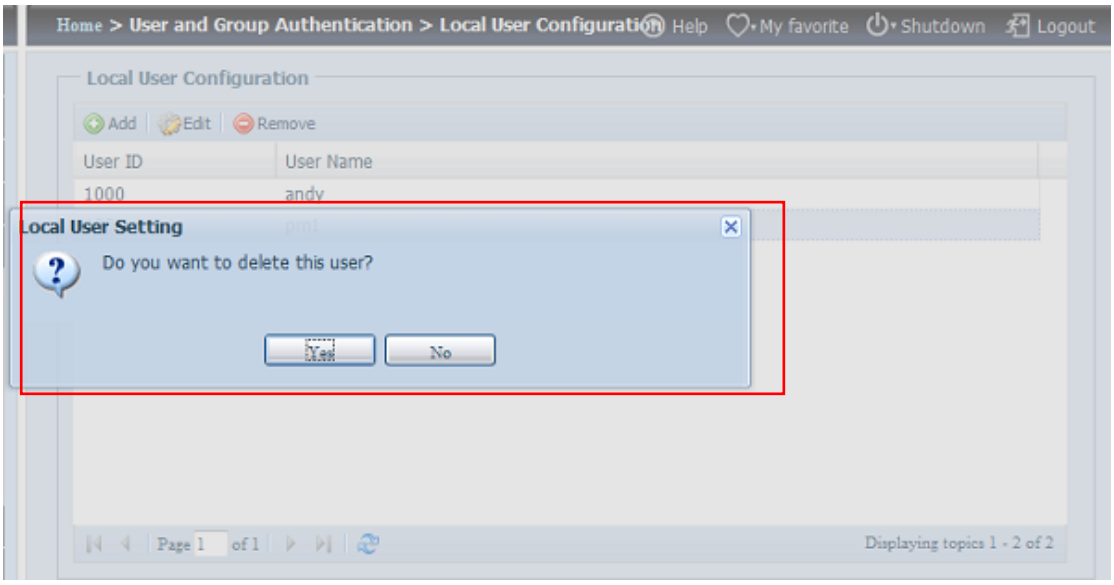
Edit Users

1. Select an existing user from the **Local User Configuration** screen.
2. Click on the ***Edit*** button, and the **Local User Setting** screen appears.
3. From here, you can enter a new password and re-enter to confirm, or use the **<<** or **>>** buttons to have this user join or leave a group. Click the ***Apply*** button to save your changes.



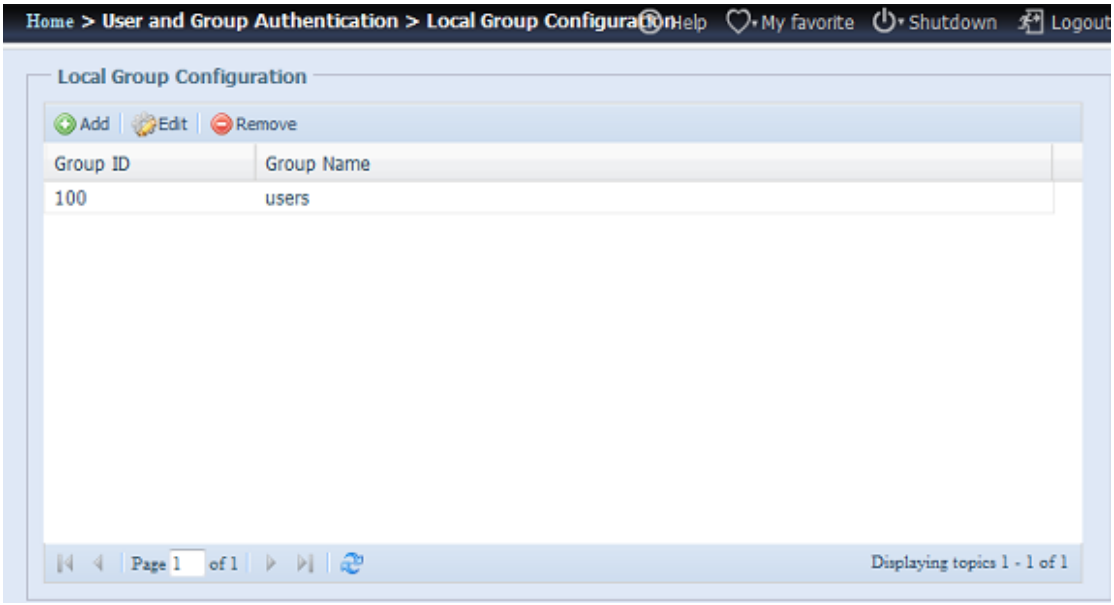
Remove Users

1. Select an existing user from the **Local User Configuration** screen.
2. Click on ***Remove*** button and the user is deleted from the system.



Local Group Configuration

From the **Accounts** menu, choose the ***Group*** item, and the **Local Group Configuration** screen appears. This screen allows you to **Add**, **Edit**, and **Remove** local groups.

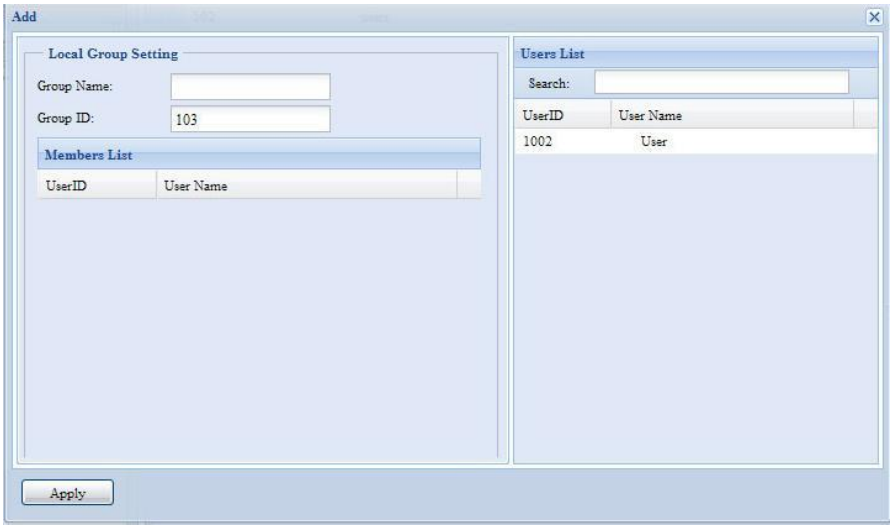


Local Group Configuration	
Item	**Description**
Add	Press the ***Add*** button to add a user to the list of local groups.
Edit	Press the ***Edit*** button to modify a selected group from the system.
Remove	Press the **Remove** button to delete a selected group from the system.

Add Groups

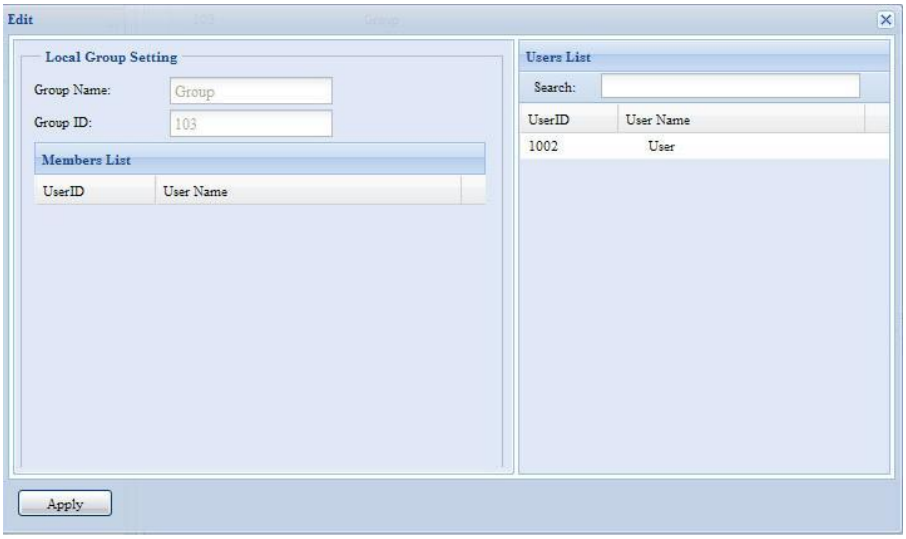
1. On the **Local Group Configuration** screen, click on the ***Add*** button.
2. The **Local Group Setting** screen appears.
3. Enter a **Group Name**.
4. Enter a **Group ID** number. If left blank, the system will automatically assign one.

5. Select users to be in this group from the **Users List** by adding them to the **Members List** using the **<<** button.
6. Click the ***Apply*** button to save your changes.



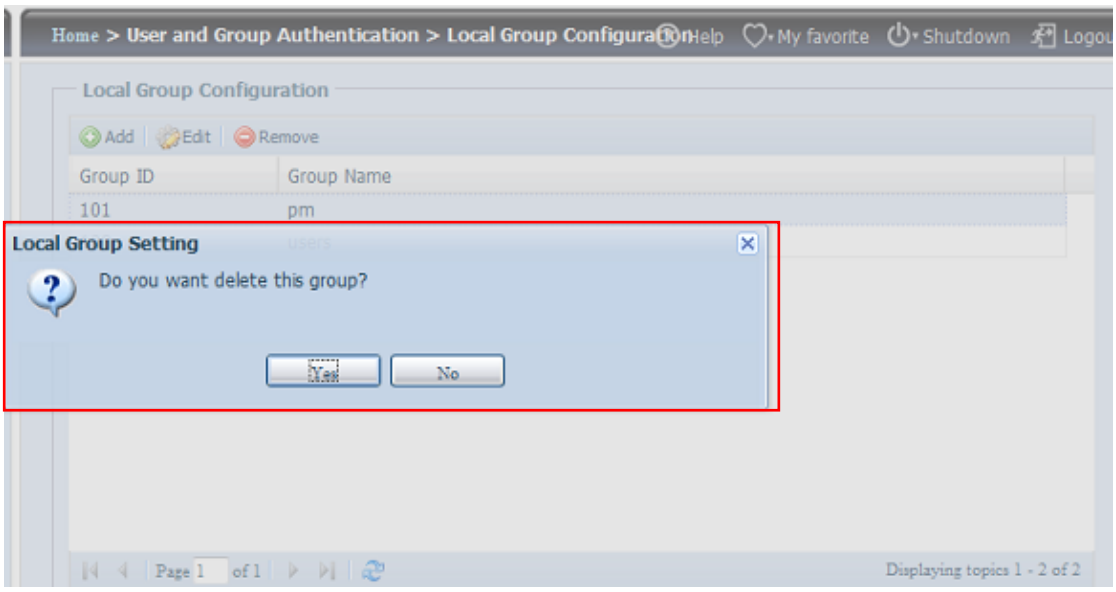
Edit Groups

1. On the **Local Group Configuration** screen, select a group name from the list.
2. Press the ***Edit*** button to modify the members in a group.
3. To add a user into a group, select the user from the **Users List**, and press the **<<** button to move the user into the **Members List**.
4. To remove a user from a group, select the user from **Members List**, and press the **>>** button.
5. Click the ***Apply*** button to save your changes.



Remove Groups

1. On the **Local Group Configuration** screen, select a group name from the list.
2. Press ***Remove*** to delete the group from the system.



Batch Users and Groups Creation

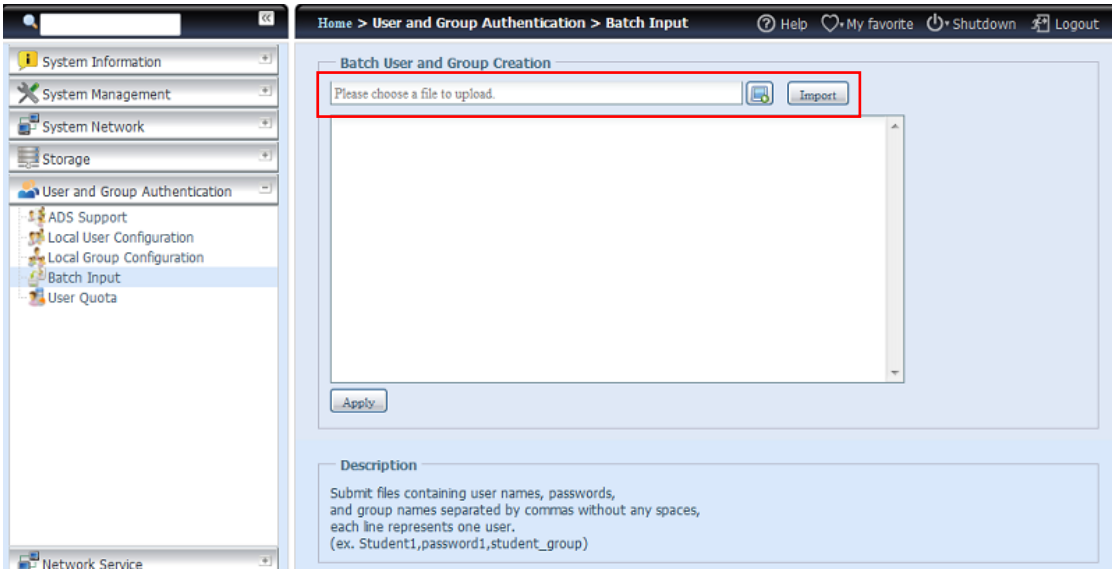
The Thecus IP storage can also add users and groups in batch mode. This enables you to conveniently add numerous users and groups automatically by importing a simple comma-separated plain text (*.txt) file.

From the **Accounts** menu, click ***Batch Input*** and the **Batch User and Group Cration** dialogue will appear. To import your list of users and groups, follow these steps:

1. Click the ***Browse*** icon to locate your comma-separated text file.
   The information in the text file should follow this format:

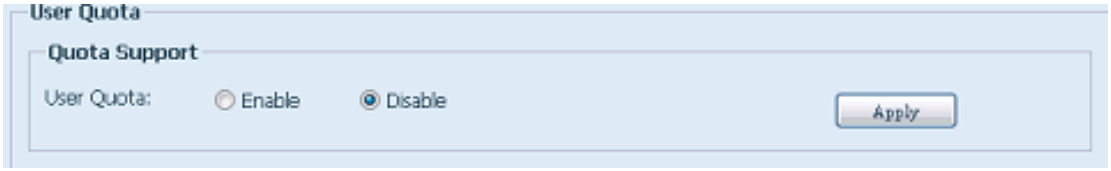
   ```
   [USERNAME], [PASSWORD], [GROUP]
   ```

2. Click ***Open***.
3. Click ***Import*** to begin the user list import.

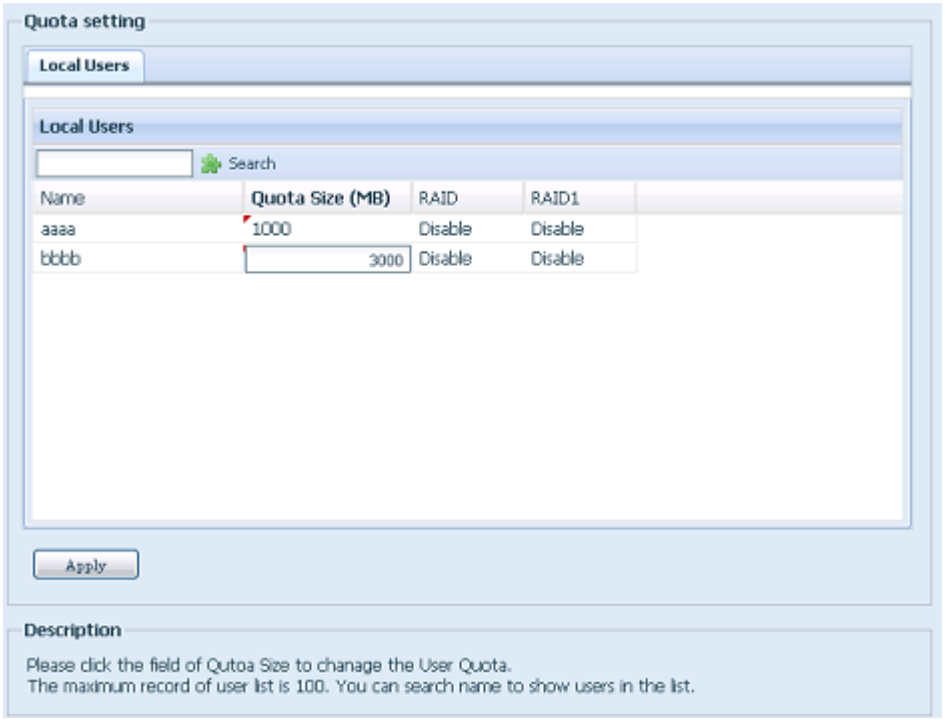


User Quota

The Thecus IP storage support local or AD users with storage quota limitations in each RAID volume of the system. To enable this function, simply click "Enable", then apply.



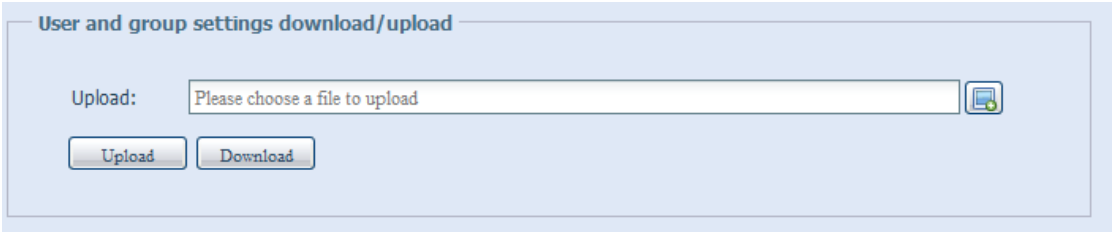
Next, each user can be setup a global storage quota size for each RAID volume. Simply click on "Quota Size" for each user and input the desired capacity. After the setup is complete, please click on "Apply" to activate the user quota size.



User and Group Backup

The user and group backup feature allow system users and groups to be backed up to another location and be restored if needed.

Please note, when restoring previous backup users and groups, the current users and groups list will be replaced from this restore file's contents.



LDAP Support

The LDAP is the other way to authenticate login users who has joined LDAP server, fill in the LDAP server information and get LDAP authentication started. Please make sure that the LDAP server has a Samba sam **and** a POSIX ObjectClass account.

A description of each item follows:

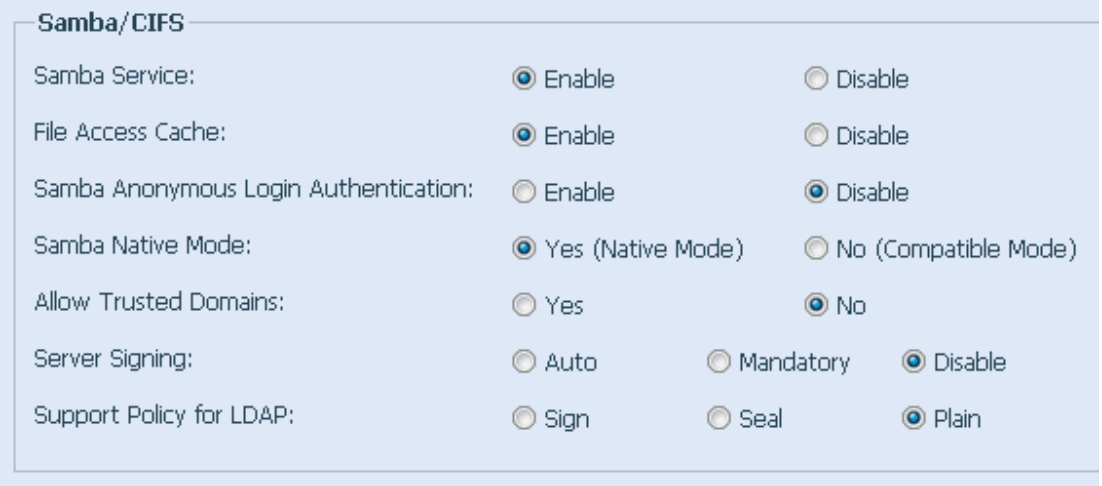
LDAP Support	
Item	**Description**
LDAP Service	**Enable** or **Disable** LDAP service.
LDAP Server IP	Input LDAP server IP address.
Base Domain	Input base domain information ex. dc=tuned, dc=com, dc=tw
Manager	Input manager's name.
Password	Input manager's password
Apply	Click ***Apply*** to save your changes.
Check ObjectClass	Click this checkbox to ensure LDAP server has a Samba sam and a POSIX account or it may not work properly for LDAP client authentication.

Network Service

Use the **Network** Service menu to make network service support settings.

Samba / CIFS

There are options allow Admin to Enable/Disable to operate Thecus IP storage associated with Samba / CIFS protocol. With the option changed, it will need to reboot system to activate.



Samba Service

Used for letting the operating system of UNIX series and SMB/CIFS of Microsoft Windows operating system (Server Message Block / Common Internet File System).Do the link in network protocol. Enable or Disable SMB/CIFS protocol for Windows, Apple, Unix drive mapping.

NOTE

- In some environments, due to security concerns, you may wish to disable SMB/CIFS as a precaution against computer viruses.

File Access Cache

File Access Cache is default **Enable**. This option will help to increase the performance while single client access share folder in writing under SMB/CIFS protocol.

Samba Anonymous Login Authentication

To enable this option, no matter there is share folder has been created in public access. The user account and password is needed from system to access under SMB/CIFS protocol. On the other hand, no more anonymous login is allowed.

Samba is Native mode

The Thecus IP storage is supported Samba mode options. In the ADS environment with "Native" mode selected then Thecus IP storage is capable to become local master position.

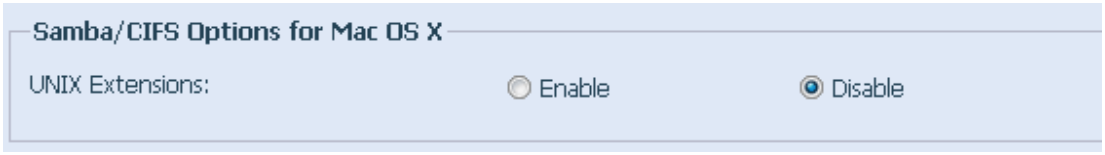
Optimize Block Size

This function controls the behavior of Samba when reporting available disk space. This function was added to allow advanced administrators to increase block size to increase write performance without re-compiling the code.

Disabled= 4k Enabled=256k

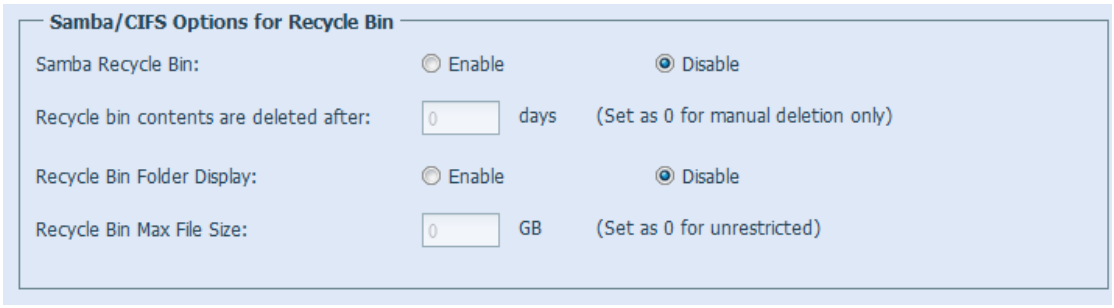
Server Signing

This is setting while Samba server has been used in US of FDCC. If the system has used only in Windows environment choose "Mandatory" otherwise "Auto".



UNIX Extension

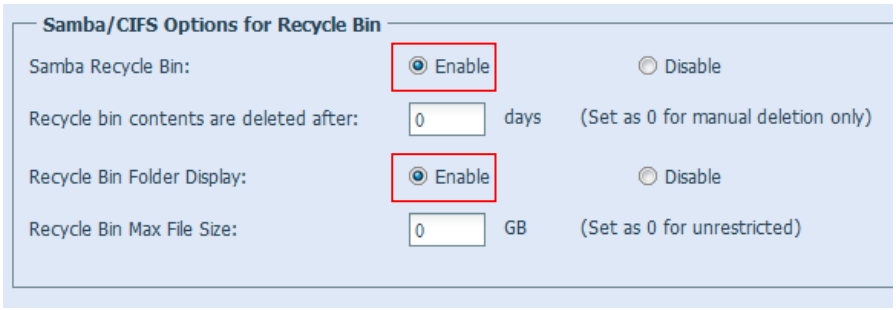
The default is enable for Samba usage, with situation using Mac OSX with smb connection may have permission issue. When it happened, please setup "UNIX Extension" disable to get issue solved.



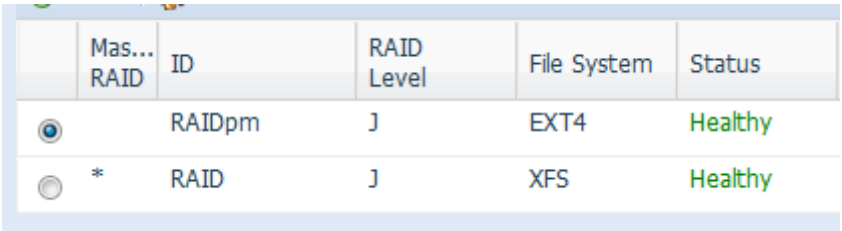
Samba Recycle Bin

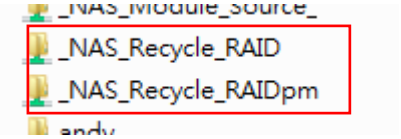
The Thecus IP storage is supported recycle bin via SMB/CIFS protocol.

Simply enable the "Recycle Bin" function and "Recycle Folder Display" then all of deleted files/folders will reside in the "_NAS_Recycle_(Associated RDID Volume)" share folder.



For example, the system has created 2 RAID volumes with ID "RAIDpm" and 'RAID". Then it will have 2 recycle bin folder appear as "_NAS_Recycle_RAID" and "_NAS_Recycle_RAIDpm".





There are 2 more setting could help to manage the recycle bin for deleted folders/files.

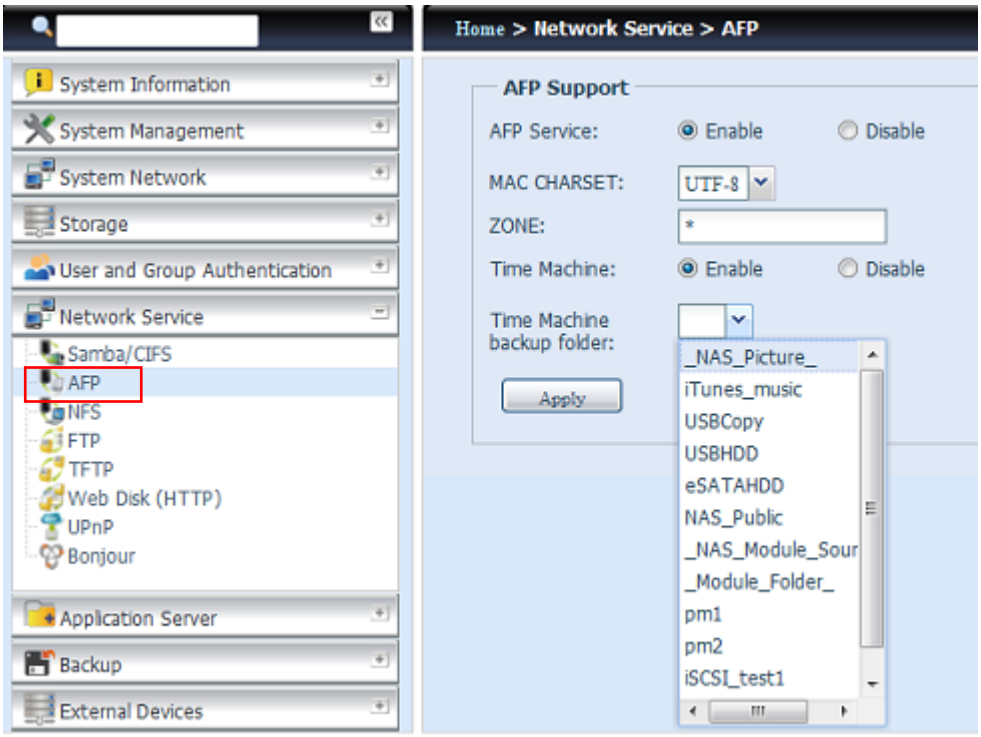
1. Setup the "Day" to remove deleted folders/files which has resided in recycle bin permanently. Left default value "0" if desired to clean up recycle bin manually.
2. Setup the "Size" for recycle bin to allow deleted folders/files can store. Left default value "0" with no limitation.

NOTE

- The deleted files/folders which have resided in recycle bin will keep its permission. On the other hand, only the admin and owner can view/read/write these folders/files.
- If deleted single file size is large than 2GB then it won't reside in the recycle bin but erase permanently.

AFP (Apple Network Setup)

From the **System Network** menu, choose the ***AFP*** item, and the **AFP Support** screen appears. This screen displays the configuration items for the Apple Filing Protocol. You can change any of these items and press ***Apply*** to confirm your settings.



A description of each item follows:

Apple Network Configuration	
Item	**Description**
AFP Server	Enable or disable Apple File Service to use the Thecus IP storage with MAC OS-based systems.
MAC CHARSET	Specifies the code page from the drop down list.
Zone	Specifies Zone for Applet Talk service. If your AppleTalk network uses extended networks and is assigned with multiple zones, assign a zone name to the Thecus IP storage. If you do not want to assign a network zone, enter an

	asterisk (*) to use the default setting.
Time Machine	Click the enable checked box if you would like your MAC system to use the Thecus IP storage as MAC time machine backup.
Time Machine backup folder	Select from the drop down list to designate the folder for time machine backup destination.

NFS Setup

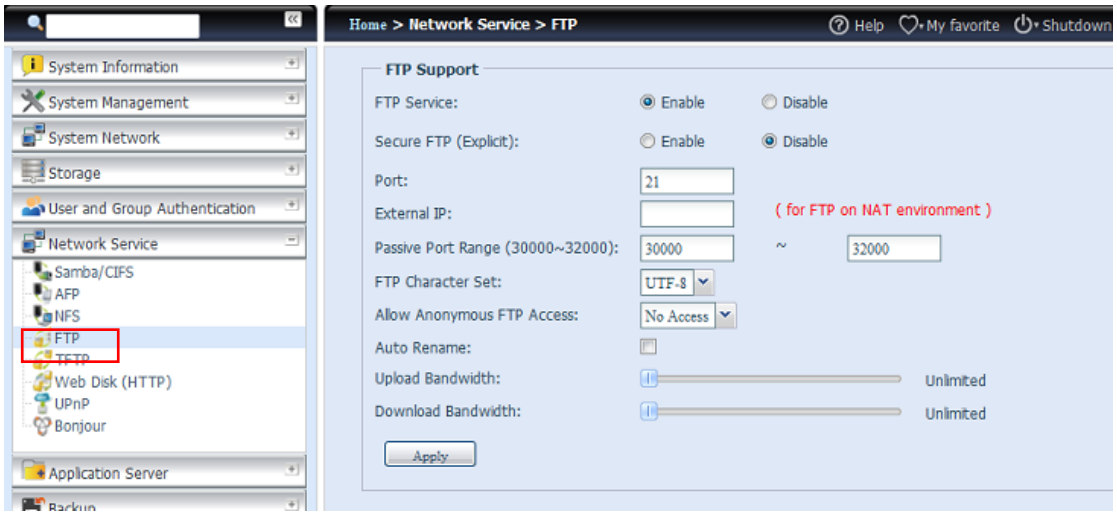
From the **System Network** menu, choose the ***NFS*** item, and the **NFS Support** screen appears. The Thecus IP storage can act as an NFS server, enabling users to download and upload files with their favorite NFS clients. Press ***Apply*** to confirm your settings.

A description of each item follows:

NFS Server Setting	
Item	**Description**
NFS	**Enable** or **Disable** NFS support.
Apply	Click ***Apply*** to save your changes.

FTP

The Thecus IP storage can act as an FTP server, enabling users to download and upload files with their favorite FTP programs. From the **System Network** menu, choose the ***FTP*** item, and the **FTP** screen appears. You can change any of these items and press ***Apply*** to confirm your settings.



A description of each item follows:

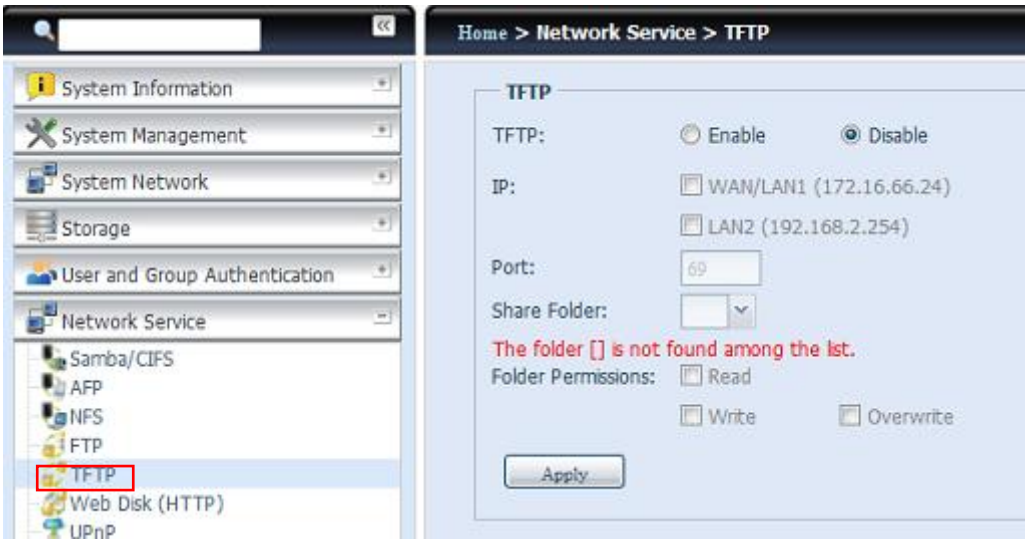
FTP	
Item	**Description**
FTP	Enables FTP Service on the Thecus IP storage.

Security FTP	Enable or disable Security FTP, be sure the client FTP software has also security FTP setting enabled.
Port	Specifies the port number of an incoming connection on a non-standard port.
External IP	Input the public IP address of the router when the Thecus secure FTP server has been enabled. This can help to respond to the ftp client with proper communication information.
Passive Port Range (30000-32000)	Limited port range for the FTP server to use.
FTP ENCODE	If your FTP client or operating system does not support Unicode (e.g. Windows® 95/98/ME or MAC OS9/8), select the same encoding as your OS here in order to properly view the files and directories on the server. Available options are BIG5, HZ, GB2312, GB18030, ISO, EUC-JP, SHIFT-JIS and UTF-8.
Allow Anonymous FTP Access	**Upload/Download:** Allow anonymous FTP users to upload or download files to/from public folders. **Download:** Allow anonymous FTP users to download files from public folders. **No access:** Block anonymous FTP user access.
Auto Rename	If checked, the system will automatically rename files that are uploaded with a duplicate file name. The renaming scheme is `[filename].#`, where # represents an integer.
Upload Bandwidth	You may set the maximum bandwidth allocated for file uploads. Selections include **Unlimited, 1 ~ 32 MB/s.**
Download Bandwidth	You may set the maximum bandwidth allocated for file downloads. Selections include **Unlimited, 1 ~ 32 MB/s.**

To access the share folder on the Thecus IP storage, use the appropriate user login and password set up on the **Users** page. Access control to each share folder is set up on the **ACL** page (***Storage Management*** > **Share *Folder*** > ***ACL***).

TFTP

Thecus IP storage can act as a TFTP server, enabling users to download and upload files with their favorite TFTP programs. From the **System Network** menu, choose the ***TFTP*** item, and the **TFTP** screen appears. You can change any of these items and press ***Apply*** to confirm your settings.



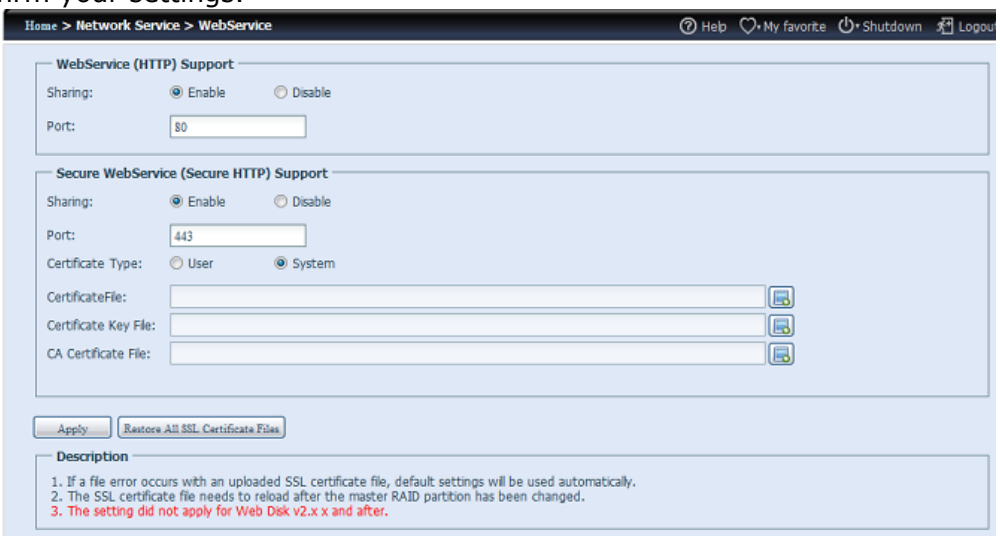
A description of each item follows:

TFTP

Item	Description
TFTP	Enables TFTP Service on the Thecus IP storage.
IP	Checked WAN/LAN1 or LAN2 to enable port use
Port	Specifies the port number of an incoming connection on a non-standard port.
Share Folder	Select the file stored folder, it cannot be empty.
Folder Permission	Select the folder permission

WebService

From the **Network Service** menu, choose the **WebService** item, and the **WebService Support** screen appears. This screen displays the service support parameters of the system. You can change any of these items and press ***Apply*** to confirm your settings.



A description of each item follows:

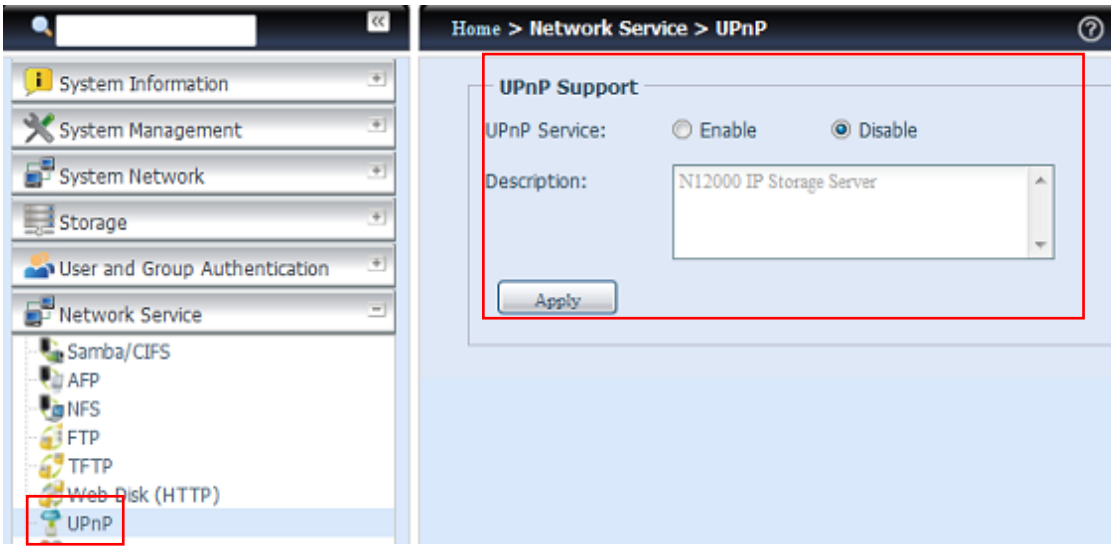
Web Service	
Item	**Description**
HTTP (WebDisk) Support	Enable or disable WebDisk support. Enter the port number if this option is enabled. The port number is default 80.
HTTPs (Secure WebDisk) Support	Enable or disable secure WebDisk support. Enter the port if this option is enabled.
Certificate Type	Select "User" if there is available Certification ID ex. Apply from VeriSign. Or using system default by select "System".
Certificate File	Upload Certificate File if choose Certificate type "User".
Certificate Key File	Upload Certificate Key File if choose Certificate type "User".
CA Certificate File	Upload CA Certificate File if choose Certificate type "User".
Restore All SSL Certificate Files	Click to set back to default certification details.
Apply	Click "Apply" to confirm the changes.

NOTE

- Disable HTTP support and Enable Secure HTTP support to guarantee secure access.

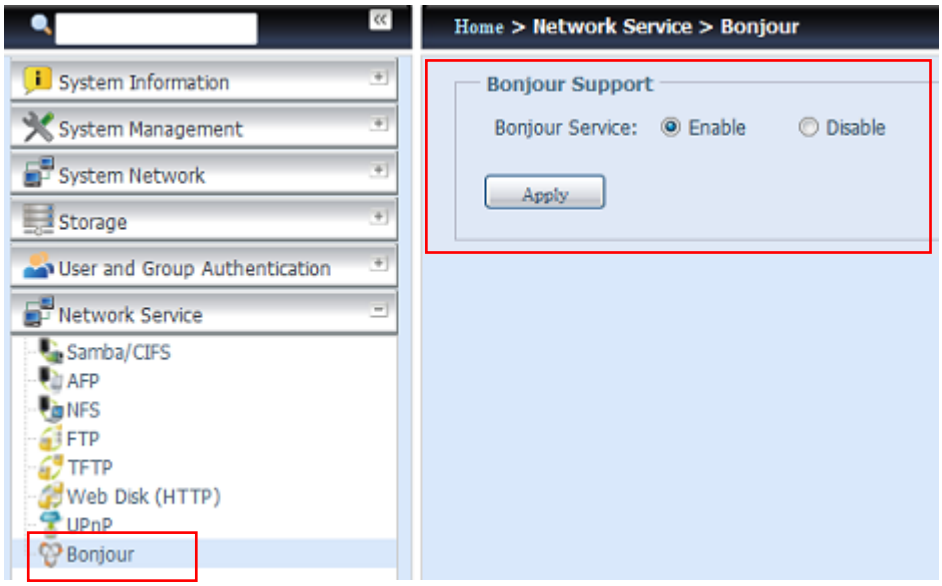
UPnP

This device supports UPnP Media server, which allows users to play media files with UPnP client (ex. DMA devices). Enable or disable Universal Plug and Play protocol. UPnP helps to find the IP address of Thecus IP storage.



Bonjour Setting

Bonjour, is Apple Inc.'s trade name for its implementation of Zeroconf, a service discovery protocol. Bonjour locates devices such as printers, as well as other computers, and the services that those devices offer on a local network using multicast Domain Name System service records. This definitive guide walks you through Bonjour zero-configuration networking with a complete description of the protocols and technologies used to create Bonjour enabled applications and devices.



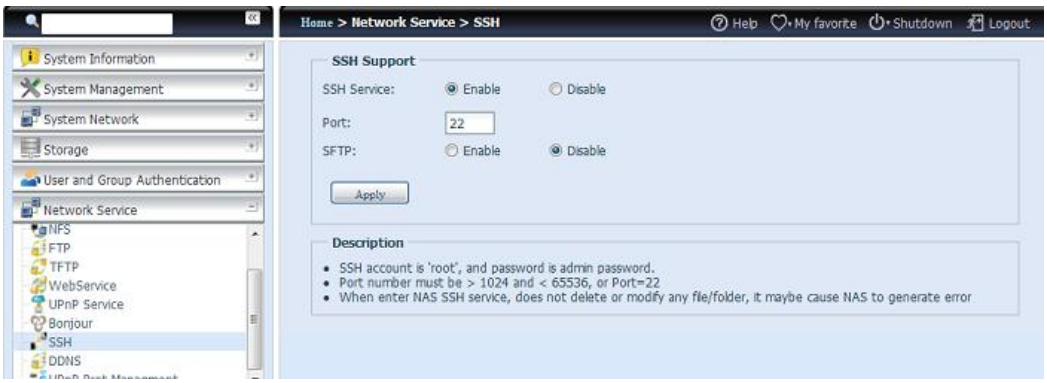
SSH

The device is now SSH protocol supported. It allows user to use SSH and have console to manipulate as needed. The SSH default login user name is “root” with full privilege and password is admin’s password. The default admin password is “admin” so once the admin password has changed then SSH login need to change the password too.

A description for each item as following:

SSH

Item	Description
SSH Service	Enable or disable SSH service.
Port	The port number is default 22.
SFTP	Enable or disable SFTP protocol under SSH service.
Apply	Click "Apply" to confirm the changes.



DDNS

To set up a server on the Internet and enable the users to connect to it easily, a fixed and easy-to remember host name is often required. However, if the ISP provides only dynamic IP address, the IP address of the server will change from time to time and is difficult to recall. You can enable the DDNS service to solve the problem.
After enabling the DDNS service of the NAS, whenever the NAS restarts or the IP address is changed, the NAS will notify the DDNS provider immediately to record the new IP address. When the user tries to connect to the NAS by the host name, the DDNS will transfer the recorded IP address to the user.
The NAS supports the DDNS providers:
DyDNS.org(Dynamic DNS),DyDNS.org(Custom DNS),DyDNS.org(Static DNS), www.zoneedit.com,www.no-ip.com.

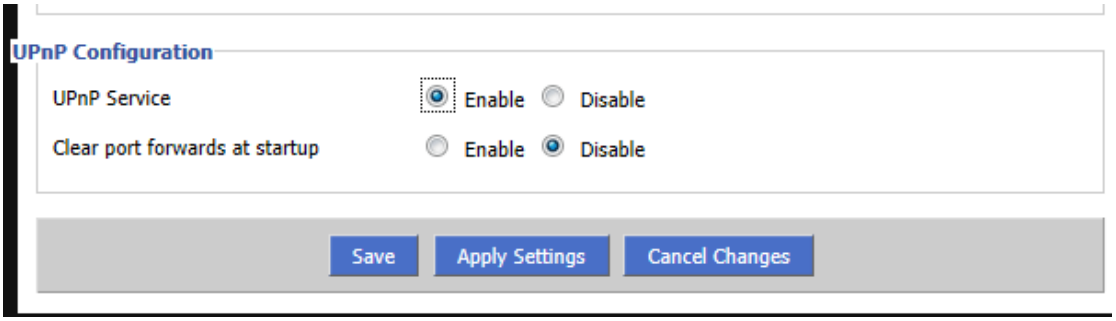
A description for each item as following:

DDNS	
Item	**Description**
DDNS Service	Enable or disable DDNS service.
Register	Choose the service provider from the drop down list
User name	Input user name with DDNS registry.
Password	Input password with DDNS registry.
Domain name	Input domain name with DDNS registry.
Apply	Click "Apply" to confirm the changes.

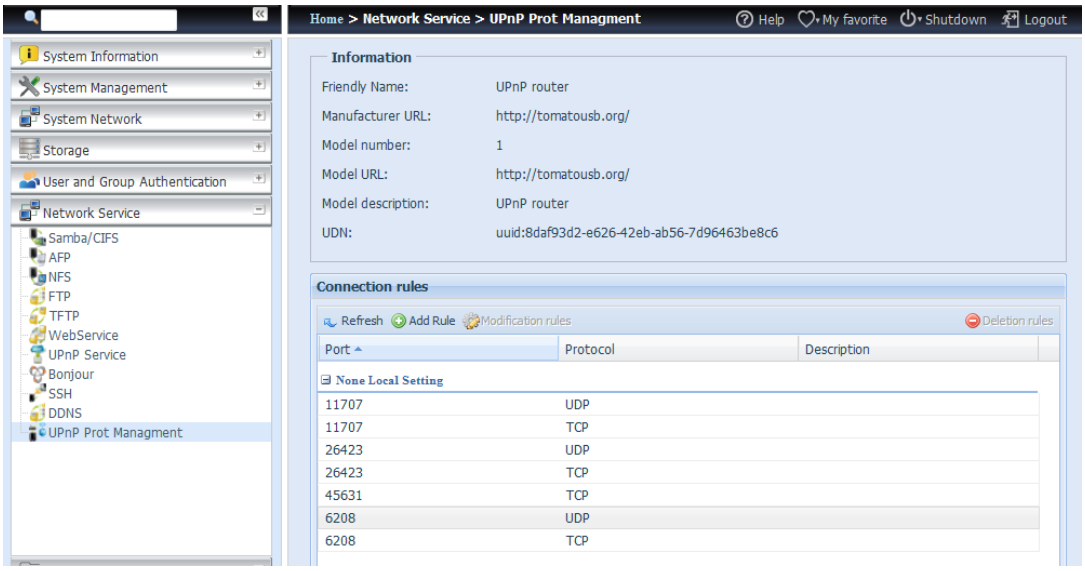
UPnP Port Management

One of the most convent way to allow users to access required services such as FTP, SSH, web disk and http etc. from Internet environment is setting UPnP port management.

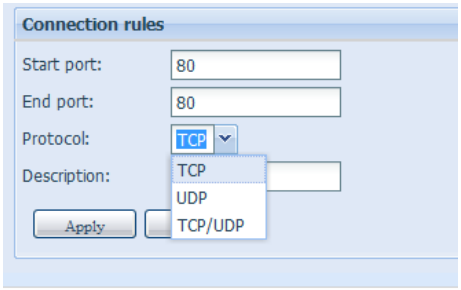
To set up this UPnP port forwarding feature, please be sure that the router has "UPnP Service" Enabled. The following is an example from one of the router manufacture with UPnP Configuration page.



After the router has enabled "UPnP Service" then you will have information come from associated router to UPnP port management as shown in the screen shot below.



And click "Add Rule" to add more port mapping from Internet to access desired services or press "Refresh" to get most updated list.



A description for each item as following:

UPnP Port Management	
Item	**Description**
Start port	Specific port number starts with.
End port	Specific port number ended
Protocol	Choose the protocol for port forwarding needed.
Description	Specific the port services if applicable.
Apply	Click "Apply" to confirm the changes.
Cancel	Click "Cancel" to abort the changes

WARNING **Some of the routers do not allow the input of port number below 1024. So it may have resulted "setting fails".**

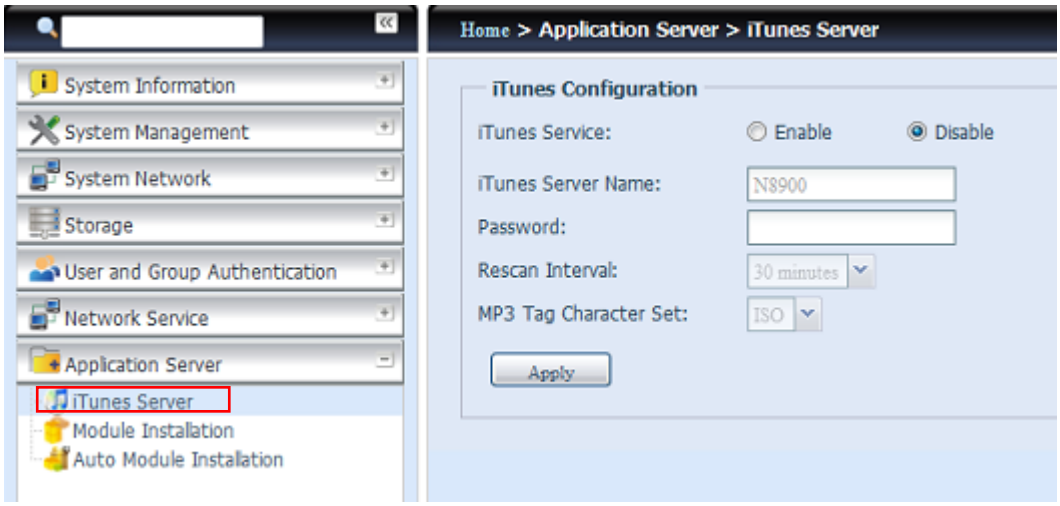
Application Server

The Thecus IP storage supports build-in application such as iTunes server. The Thecus IP storage provides activation of the iTunes Server on the device. You will be able to play music files on this device with your iTunes client software directly. The following section shows you how.

iTunes® Server

With the built-in iTunes server capability, Thecus IP storage enables digital music to be shared and played anywhere on the network!

From the **Network** menu, choose the ***iTunes*** item, and the **iTunes Configuration** screen appears. You may enable or disable the iTunes Service from here. Once enabled, enter the proper information for each field and press ***Apply*** to save your changes.



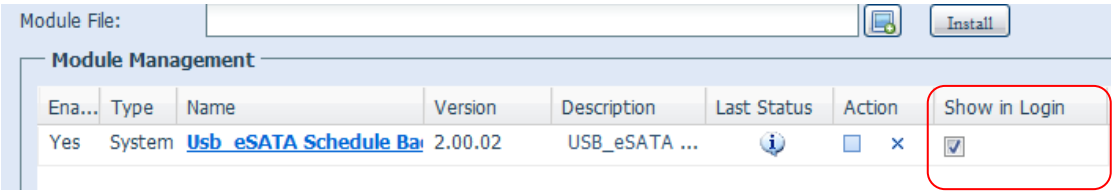
See the following table for a detailed description of each field:

iTunes Configuration	
Item	**Description**
iTunes Service	Enable or disable the iTunes Service.
iTunes Server Name	Name used to identify Thecus IP storage to iTunes clients.
Password	Enter a password to control access to your iTunes music.
Rescan Interval	Rescan interval in seconds.
MP3 Tag Encode	Specify tag encoding for MP3 files stored in Thecus IP storage. All ID3 tags will be sent out in UTF-8 format.

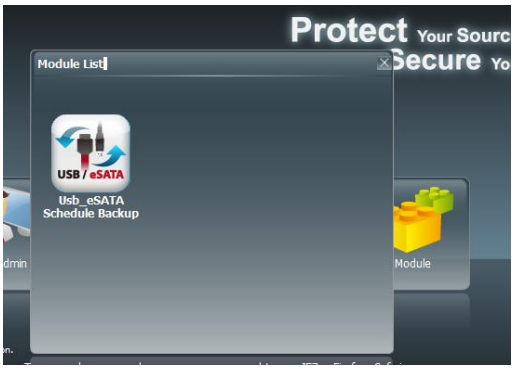
Once the iTunes service is enabled, Thecus IP storage will make all music located in the **Music** folder available for iTunes-equipped computers on the network.

Module Installation

From the login page, other than admin, web disk and Piczza (Photo server) the module icon is a newly added feature for this FW release. After a module has been installed, a new option will be available to "Show in Login".

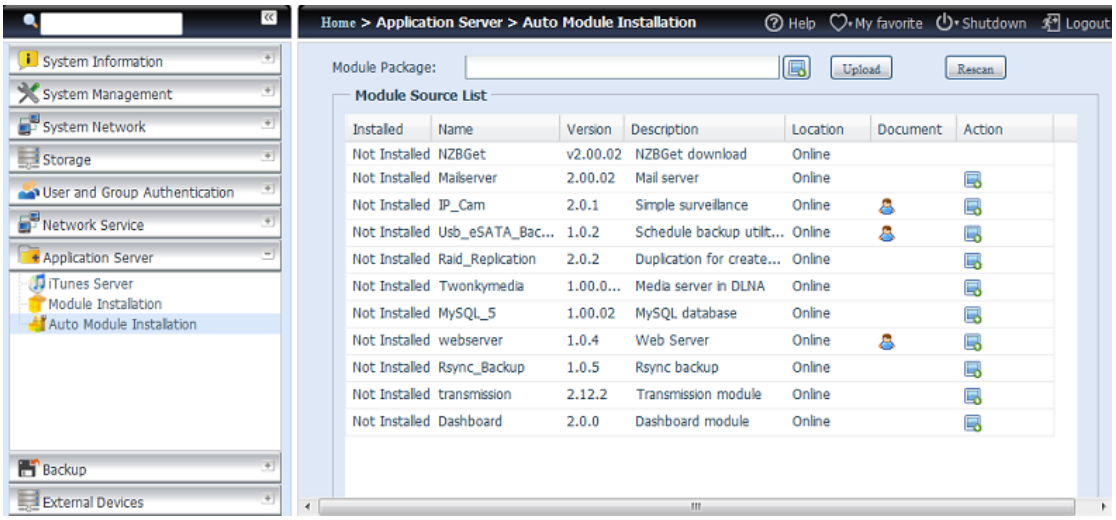


If this option is enabled then, when login to the system, the module icon will be available for all valid users to login through.



Auto Module Installation

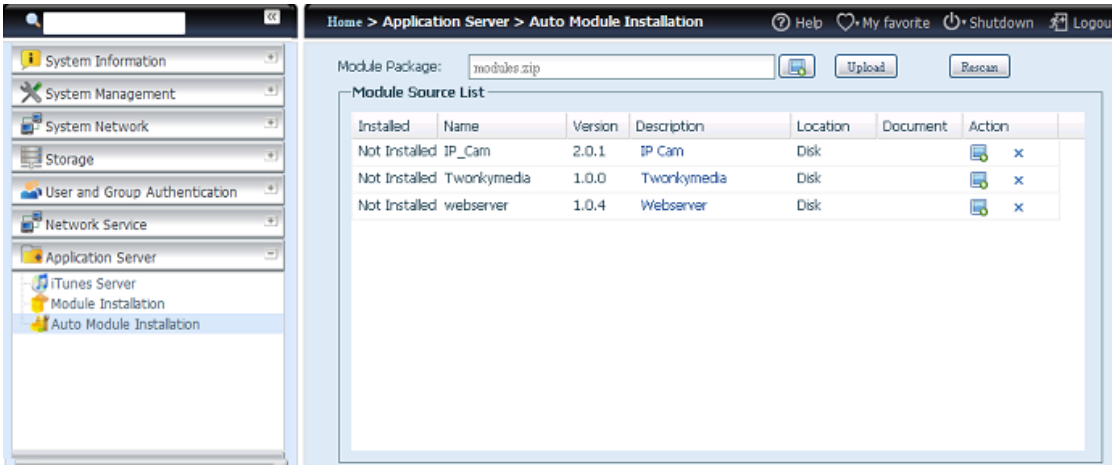
Choose the ***Auto Module Installation*** item and the **available system Module** screen appears. The default for this module list is located online. So if the Thecus IP storage is capable to connect to Internet, then it will automatically link to the Thecus official website and list the available modules. Please refer the screen shot below.


Home > Application Server > Auto Module Installation
Help
My favorite
Shutdown
Logout
System Information
System Management
System Network
Storage
User and Group Authentication
Network Service
Application Server
iTunes Server
Module Installation
Auto Module Installation
Backup
External Devices
Module Package:
Upload
Rescan
Module Source List
Installed Name Version Description Location Document Action
Not Installed NZBGet v2.00.02 NZBGet download Online
Not Installed Mailserver 2.00.02 Mail server Online
Not Installed IP_Cam 2.0.1 Simple surveillance Online
Not Installed Usb_eSATA_Bac... 1.0.2 Schedule backup utilit... Online
Not Installed Raid_Replication 2.0.2 Duplication for create... Online
Not Installed Twonkymedia 1.00.0... Media server in DLNA Online
Not Installed MySQL_5 1.00.02 MySQL database Online
Not Installed webserver 1.0.4 Web Server Online
Not Installed Rsync_Backup 1.0.5 Rsync backup Online
Not Installed transmission 2.12.2 Transmission module Online
Not Installed Dashboard 2.0.0 Dashboard module Online

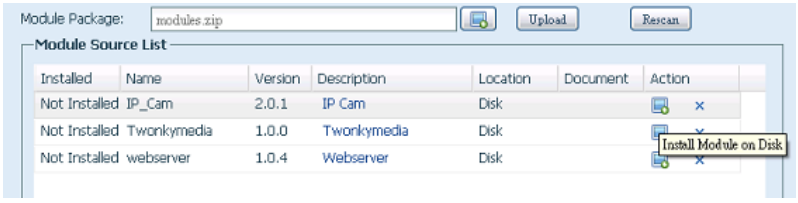
Another way to have auto module installed is to use the universal CD shipped with system. It contains a file "modules.zip" which included all the modules available when the system was shipped. Please refer the screenshot below.

NOTE

The on-line modules list from the Thecus website will be newer then than "thecus.zip" from the shipped CD. The installations performed from the Thecus website could have unpredictable duration due to bandwidth concern.



Auto Module Source List	
Item	**Description**
Installed	Status of module
Name	Module name
Version	The version of the released module
Description	The description of the module
Location	The module is either located on-line or disk
Document	The available documentation of the module
Action	To install or delete module. p.s. If the module list from on-line, then no delete option will be available
Rescan	Click to rescan from both on-line and disk



After clicking on "Action" to install a module, the module will become available under the list of Module Installation. Please go to Module installation and click "Enable" to activate the module.

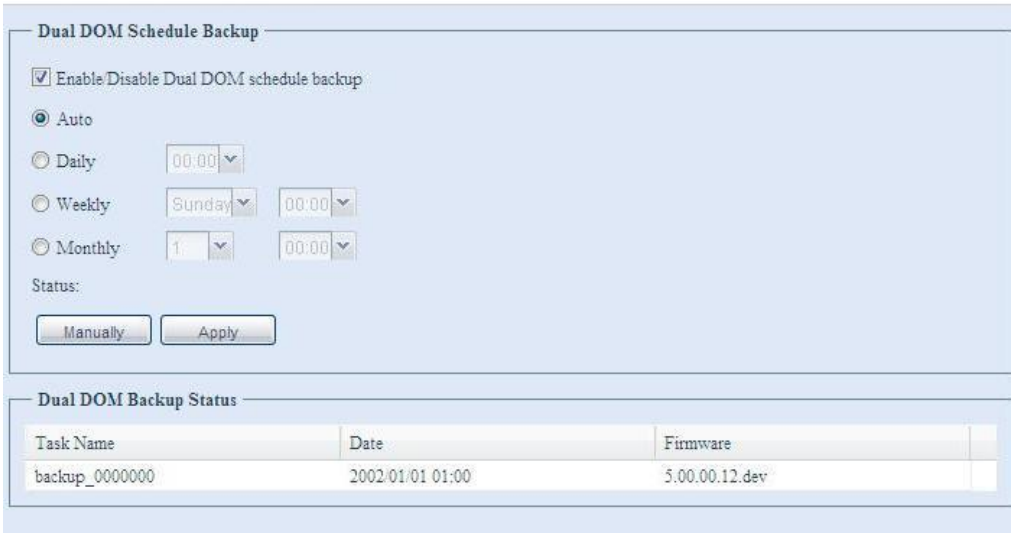
Backup

There are a number of ways to back up data with the Thecus IP storage.

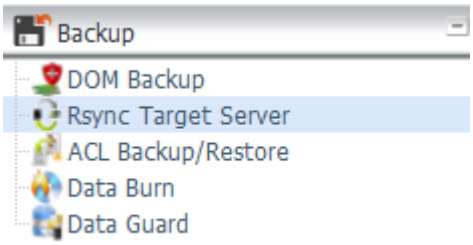
Dual DOM (N12000 series/N16000 series/N8900 series only)

The unique Dual DOM feature can now perform "Auto Repair". The Thecus NAS will backup up to five versions of the system configuration either by the default timing of 1:00am every day automatically or as scheduled by the user.

This unique "Auto Repair" will be triggered if the primary DOM has a booting issue. In this instance, the 2nd DOM will take over the boot function. Then, the system will automatically load the most recent system configuration backup image to repair the primary DOM.



Rsync Target Server

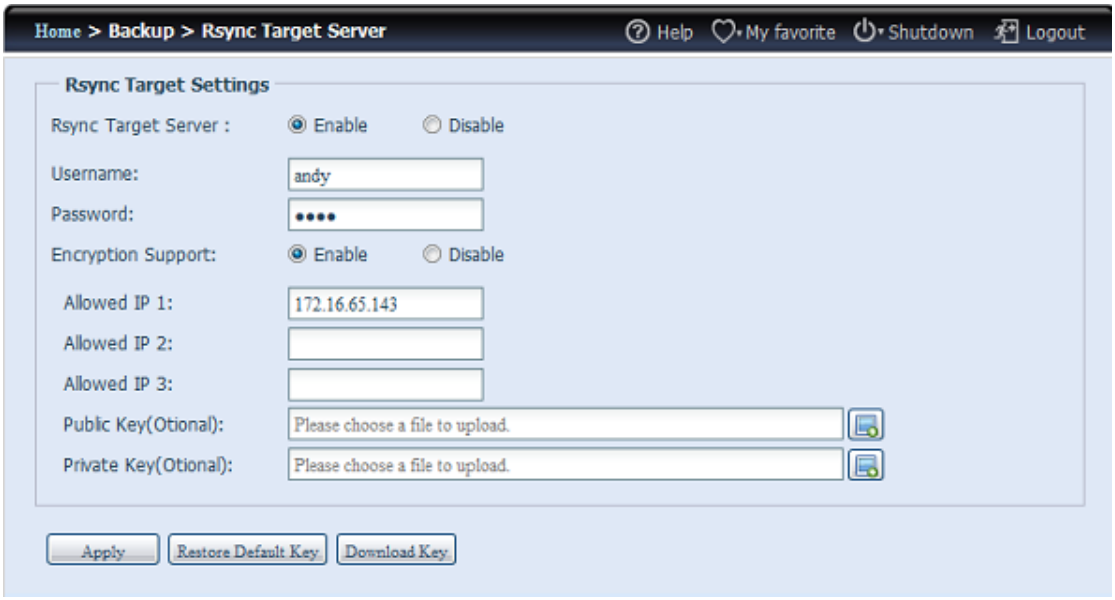


When it comes to backing up your data, it's very important to have flexibility. Data guard provides you with many options, including full backup for all shares, custom backup for selected shares and iSCSI volume backup. Being based on the Linux operating system, it is also much more stable and experiences much less frequent data loss during transfer than other remote backup systems.

-For this tutorial you will need to use Rsync Target Server (Step 1) and Data Guard (Step 2+3) under Backup for this client/server backup feature. It also can be named for function "Remote Replication".

Step 1 – Enabling Rsync on your target (backup) NAS

-Log in to your target (backup) NAS through the UI in your web browser
-Go to Rsync Target Server under Backup in the menu of the UI



1. Enable **Rsync Target Server**
2. Add a **username** and **password** (they can be different than your NAS's username and password)
3. Select **Apply**

NOTE

- You will need this user name and password while the data is going to remotely backup to this Rsync target server.

Now Rsync is turned on your NAS, which means it can be used as a target for Rsync backup, in other words, only the backup NAS needs to be activated in this way.

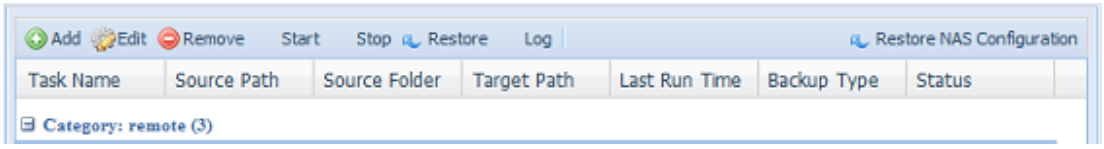
Data Guard (Remote Backup)

Step 2 – Setting up your backup task and schedule on your source NAS

-Log in to your other NAS (your source NAS) through the UI in your web browser

-Go to **Data Guard** under **Backup** in the menu of the UI

-From the **Data Guard** function list, choose **Add**

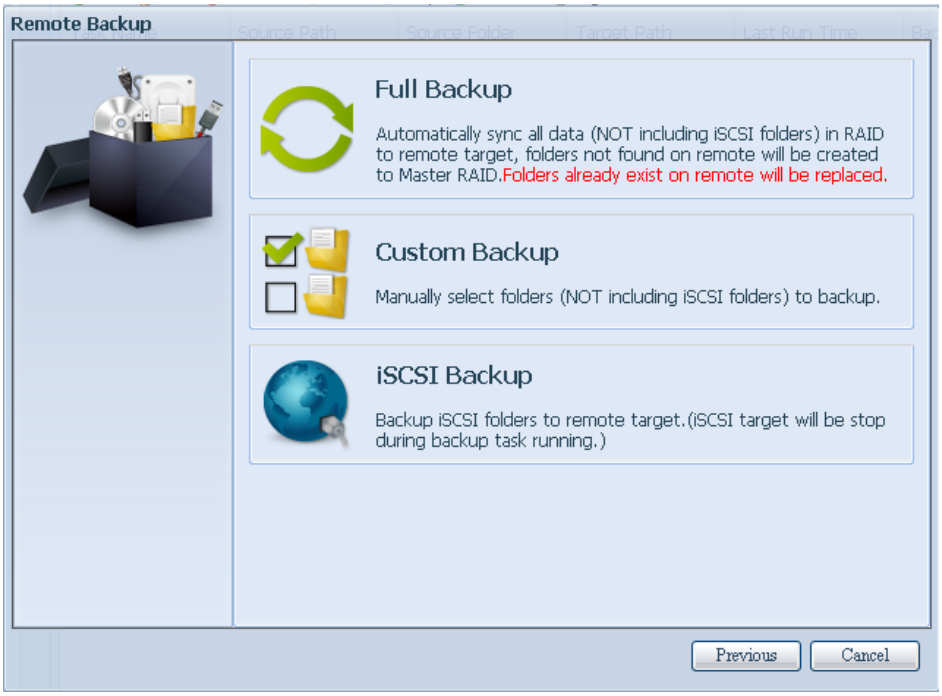


Remote Data backup	
Item	**Description**
Add	Add new task.
Edit	Edit select task.
Remove	Remove select task
Start	If associated task has been setup in schedule and like to start at once, click on to start task right away.
Stop	Stop the associated running task. The other scenario is if a task has been setup in real-time then clicking "Stop" can terminate the running process. Simple click 'Start" to

	re-start the real-time operation.
Restore	Restore the associated task
Log	Click to view the associated task in process details.
Restore NAS Configuration	Click to restore system configuration from selected destination to source unit. More details will describe in sections.

The data backup setup wizard appears as below, click on 'Remote Backup":

Then 3 different selections appear and can be chosen from:

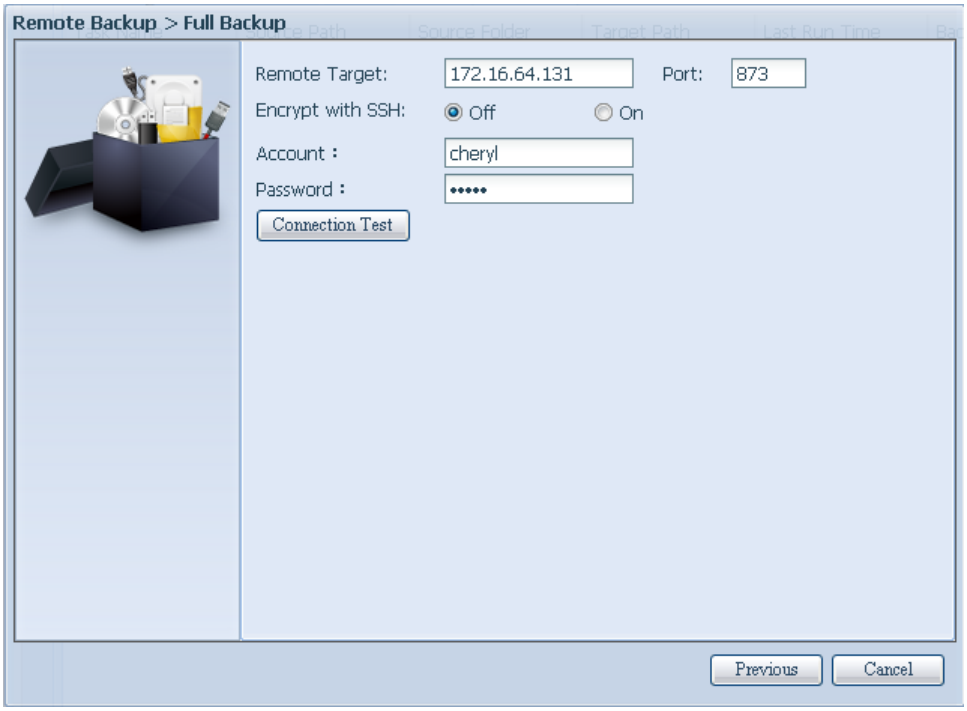

Remote Backup
Full Backup
Automatically sync all data (NOT including iSCSI folders) in RAID to remote target, folders not found on remote will be created to Master RAID.Folders already exist on remote will be replaced.
Custom Backup
Manually select folders (NOT including iSCSI folders) to backup.
iSCSI Backup
Backup iSCSI folders to remote target.(iSCSI target will be stop during backup task running.)
Previous
Cancel

Remote Data backup	
Item	**Description**
Full Backup	The "Full backup" will have all shares from source backup to

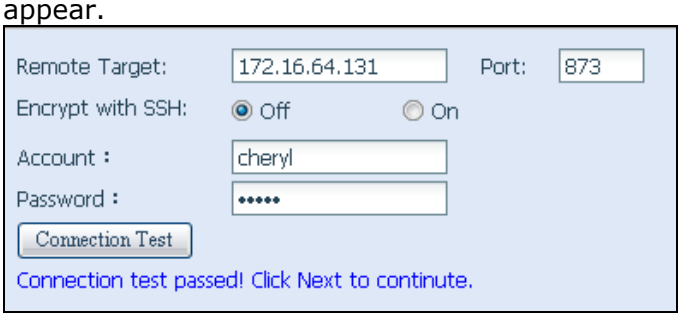
	destination. It could also create shares automatically from destination if it is not existent. This only applies if the target server is the same model as the source.
Custom Backup	The "Custom backup" allows user to choose desired shares backup to destination.
iSCSI Backup	The "iSCSI backup" can backup iSCSI volume as single file to destination.

Full Backup

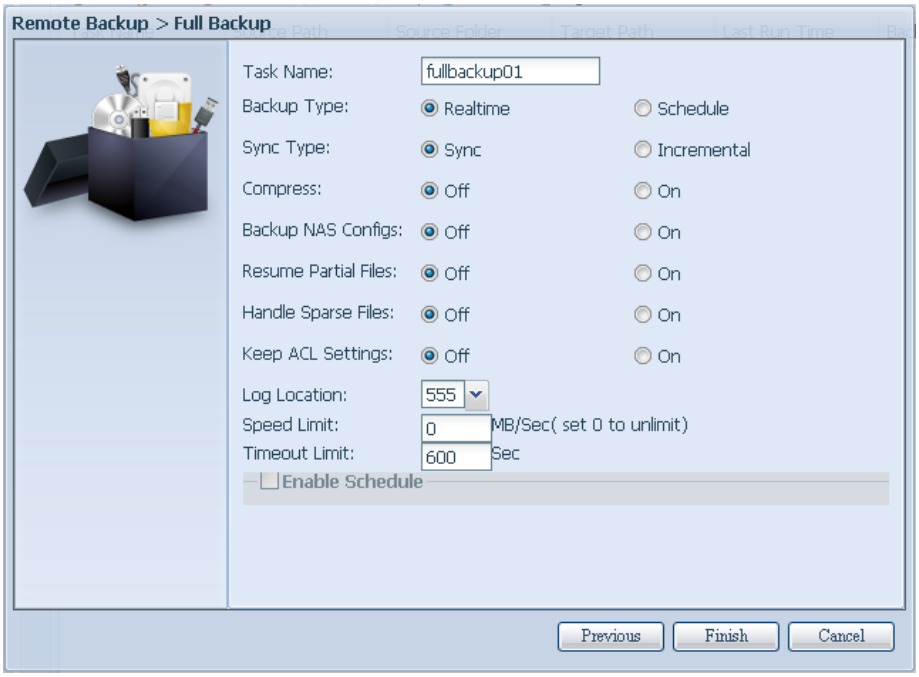
Click on full backup and the setup screen appear as below. Fill in the remote target IP (Destination) and port (need to be changed only if this port is already in use). If encryption is required then enable it. Please make sure the associated target server also has encryption enabled.
Carry on with inputting valid remote target server account name and password.



After the settings are complete, please click on "Connection Test". The source unit will try to connect with the associated target system. If a connection can be built up successfully then "Connection passed" will be prompted, otherwise "Failed" will appear.



Click "Next" and more setting will appear.

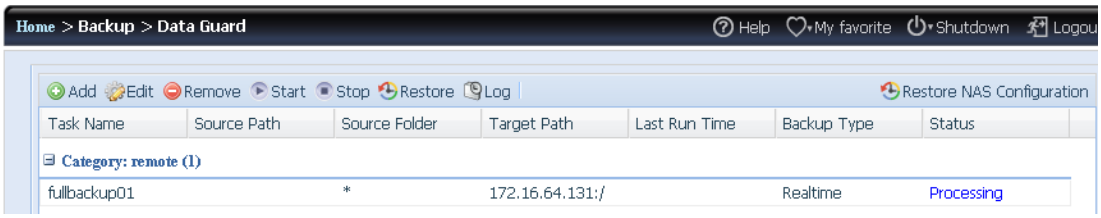


-Fill out all the necessary details and choose your parameters

Add Rsync Backup Task	
Item	**Description**
Task Name	This is how this task will appear in the task list.
Backup Type	Real time: It will backup folders/files from source to target on the fly. On the other hand, any changes from the source will back up to the target right away. Schedule: The task will start only according to the schedule.
Sync Type	Sync mode: Makes your source match your target completely; deleting and adding files on your target as they are deleted and added on your source. Incremental Mode : Makes your source match your target and keep all old files; adding files on your target as they are added on your source, but NOT deleting files on your target as they are deleted on your source.
Compress	With this option, compress the file data as it is sent to the destination machine, which reduces the amount of data being transmitted – something that is useful over a slow connection.
Backup NAS Config	Enabling this will back up the source unit system configurations to the designed path on the target system.
Resume Partial File	
Handle Sparse File	Try to handle sparse file efficiently so they take up less space on the destination.
Keep ACL Setting	It will backup not just data itself but also ACL configuration with associated folders/files.
Log Location	Choose the folder to save the log details while the task is executed.

Speed Limit	Input the bandwidth control for data backup operation.
Timeout Limit	Setup the timeout when trying to build up a connection in between the source and the target system.
Enable Schedule	If backup is set as "Schedule", please input the related period and time.

After the required fields are filled and the parameters are setup, click 'Finish" to complete. The data guard task will appear in the list as shown below.

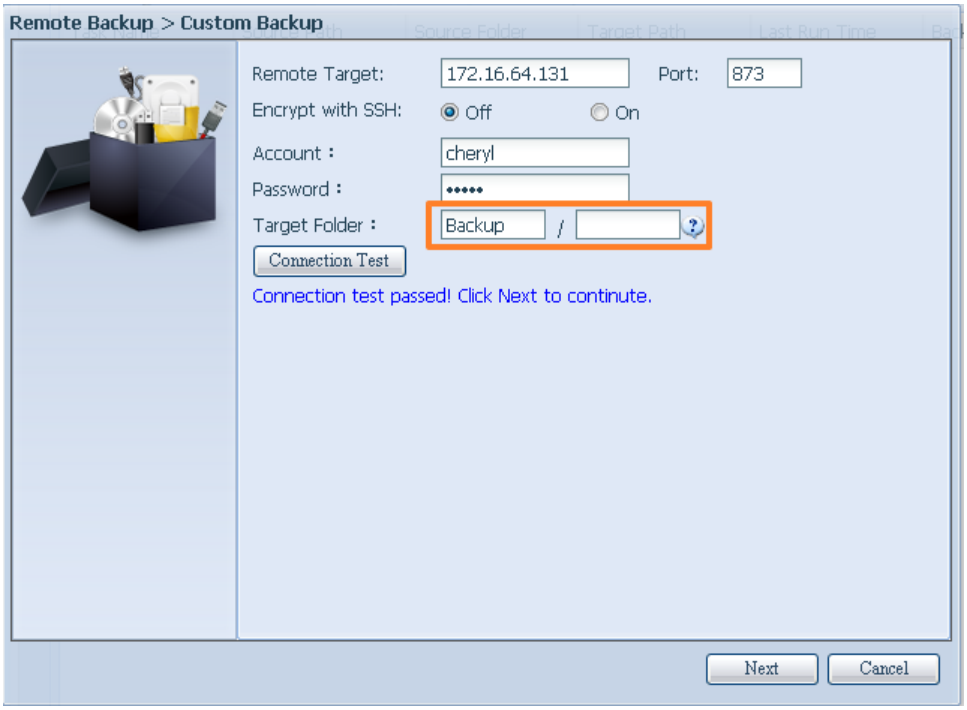


From the task list, you can now see the newly added task "fullback01". The backup is setup as "real time". From the status field, "Processing" can be read as the back-up is performed on the fly.

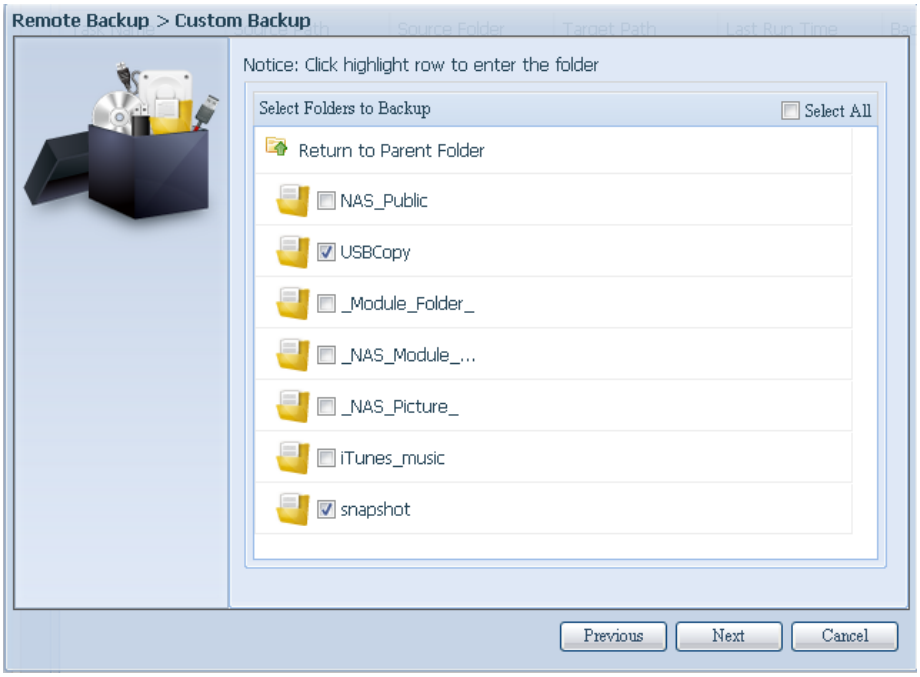
Custom Backup

The custom backup setting is similar to the full backup. The only differences are explained below:

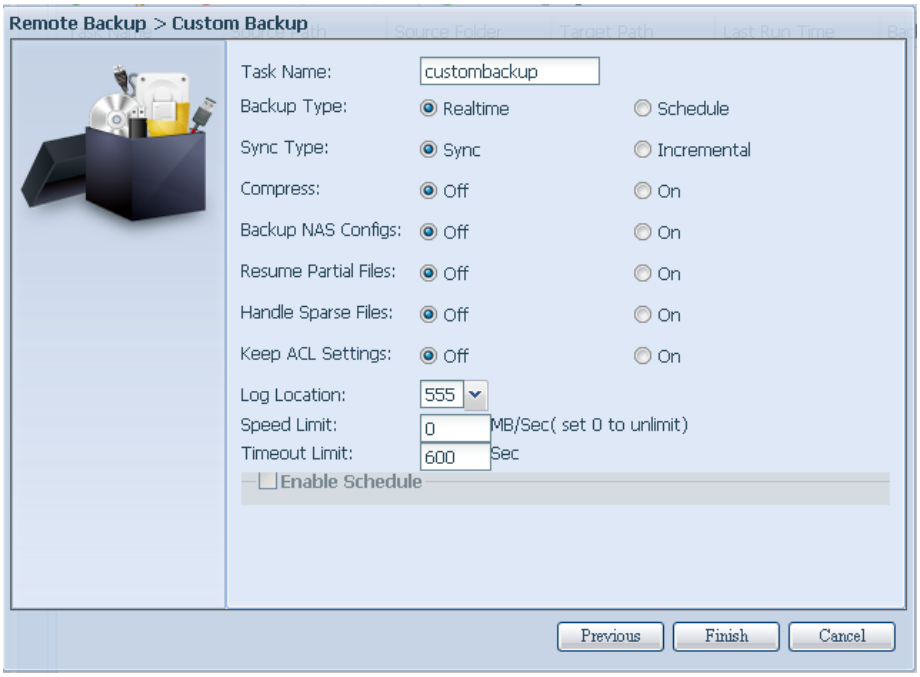
1. Inputs the share folder name of target sever where the source is going to backup. The sub-folder can be left as blank.



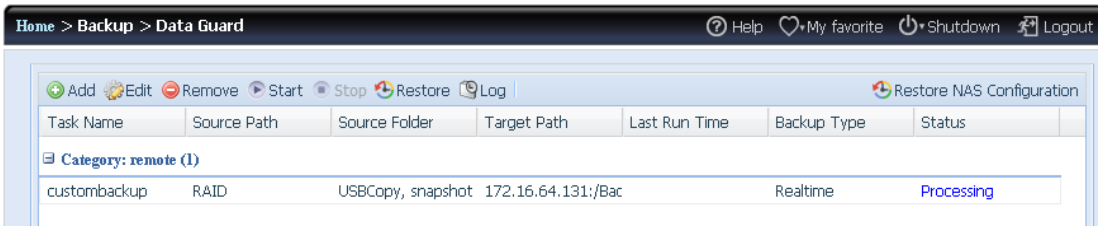
2. Select the source share folder(s) which are desired to be backed up to the target server. You can also click on "Select All" from top right corner check box.



3. Click "Next" and more setting appears. These are the as the settings for "Full backup"



4. Click "Finish" and the data guard task will appear in the list as shown below.

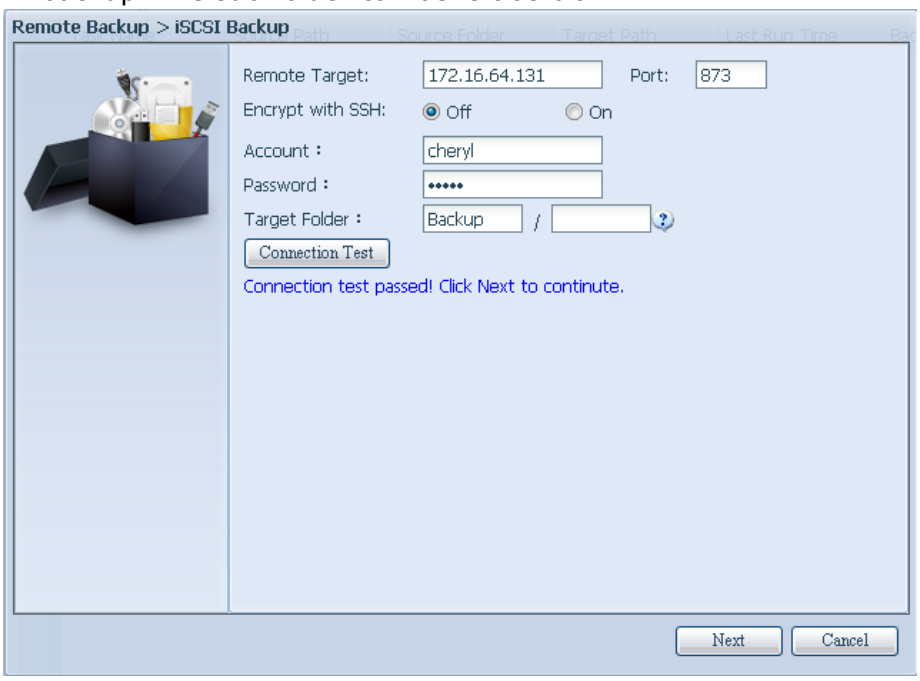


From the task list, you can now see the newly added "customback01". This backup is setup as "schedule".

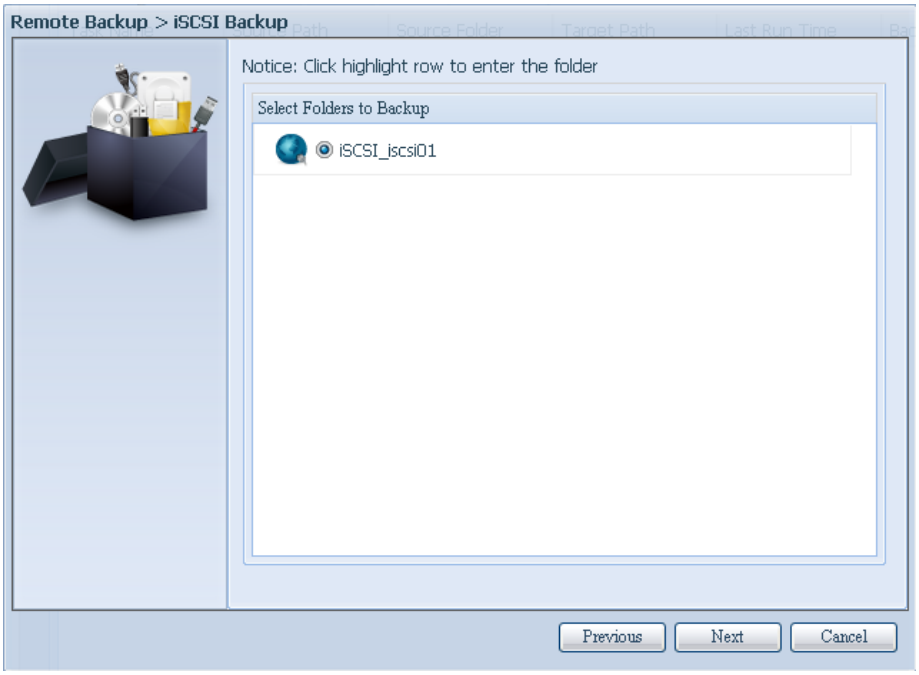
iSCSI Backup

If the source unit contains iSCSI volume, it can be backed up to the target unit as a single file. The procedure is the same as for the previous "Full backup" and "Custom backup", select "iSCSI backup" from data guard wizard.

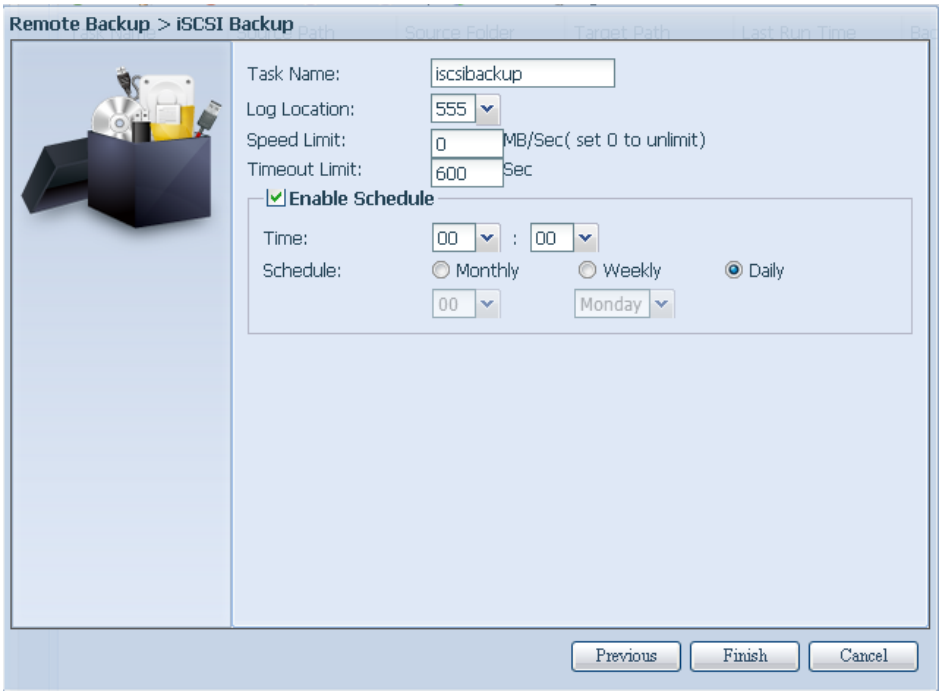
1. Inputs the share folder name of the target sever where the source is going to backup. The sub-folder can be left as blank.



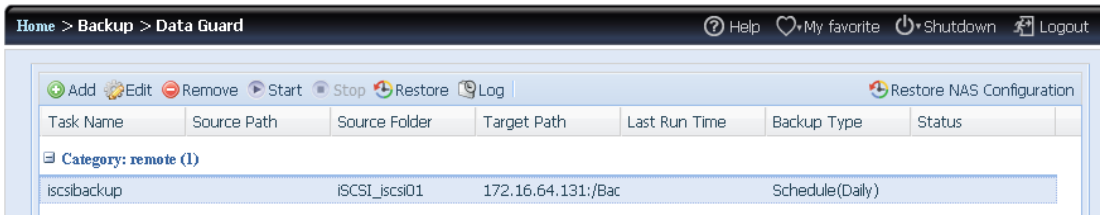
2. Select the iSCSI target volume which you wish to back up to the target server.



3. Click "Next" and more settings will appear. It is slightly differing from "Full backup" and "Custom backup". Only "Schedule" backup is supported with less options.



4. Click "Finish" and the data guard task will appear in the list as shown below.



From the task list, you can now see the newly added "iscsiback". This backup is setup as "schedule".

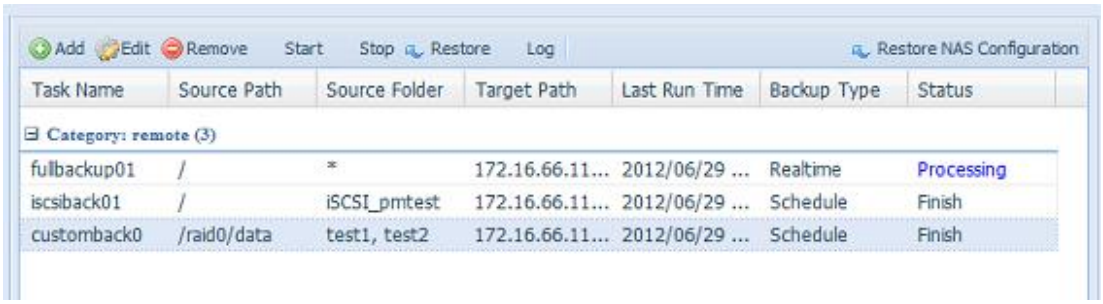
NOTE

- The source folder name will use iSCSI_+target volume name. So here it is displayed as "iSCSI_pmtest". pmtest is the iSCSI target name when the iSCSI target was created.

The iSCSI backup can see the result as below. The task "iSCSI_pmtest" has backup to target 172.16.66.131 and share folder NAS_Public with file "iSCSI_pmtest".

Restore

To restore a backup from the backup task, simply select a task from the task list then click "Restore" from the function bar. The restore task will start to have the associated files/folders from the target server restored to the source.



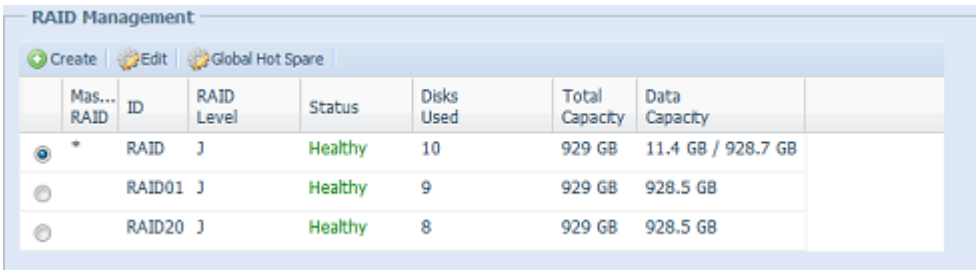
NOTE

- To restore task with backup type set as "Real time", first you need to stop the task then you can proceed with the restore operation.

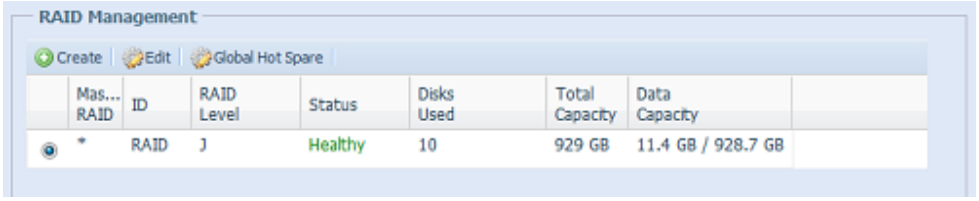
Restore NAS Configuration

This is a useful feature if the system configuration needs to be restored to a brand new unit. Let's go thru the following example to see how it works.

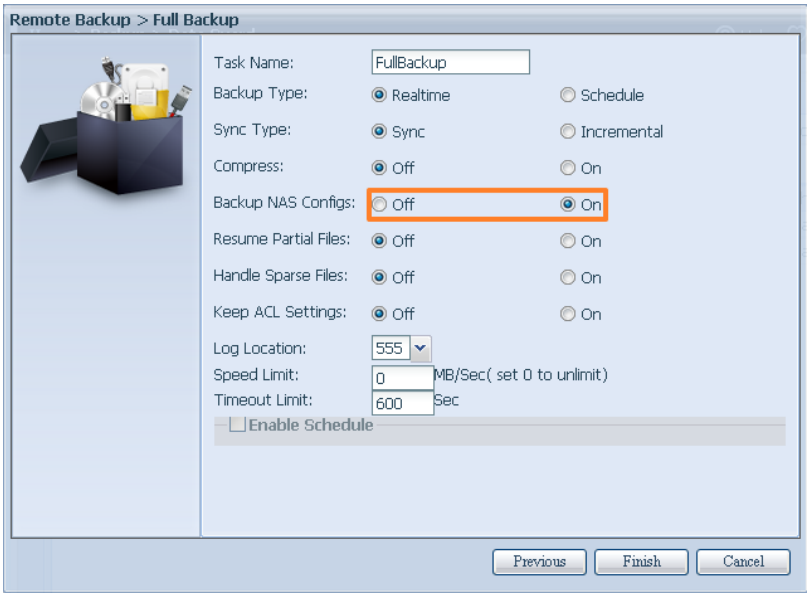
The original source system has 3 RAID volume, "RAID", 'RAID10" and "RAID20", and has backed up the system configurations to the target server.



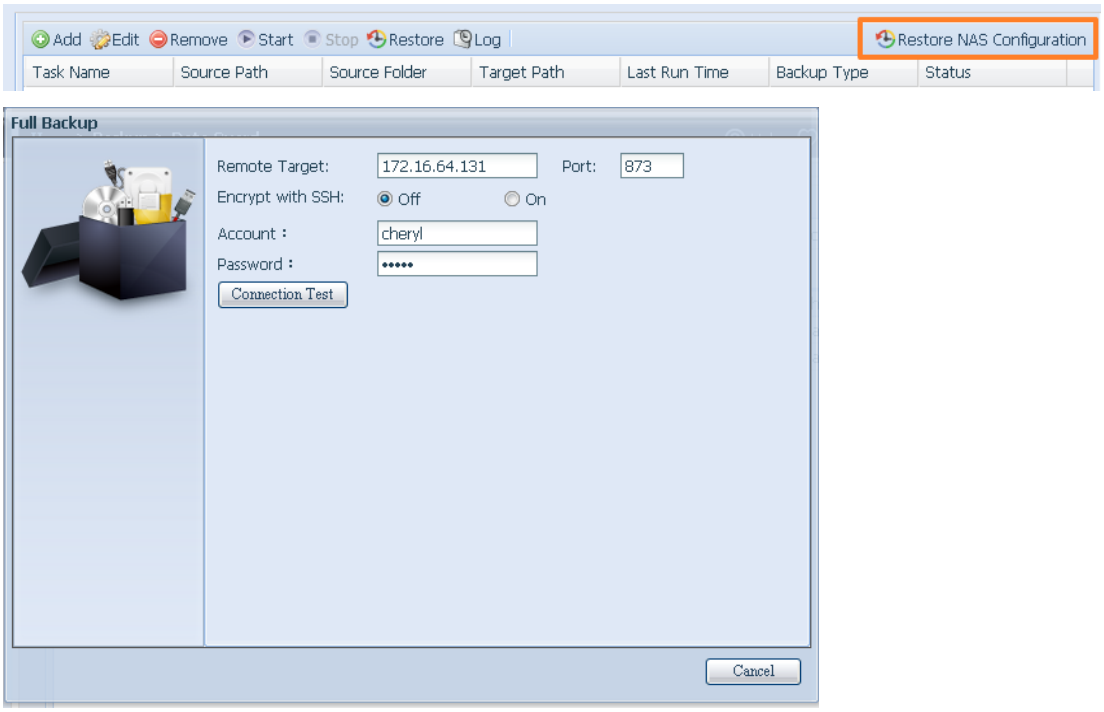
The brand new source unit only has a 1 RAID volume 'RAID".



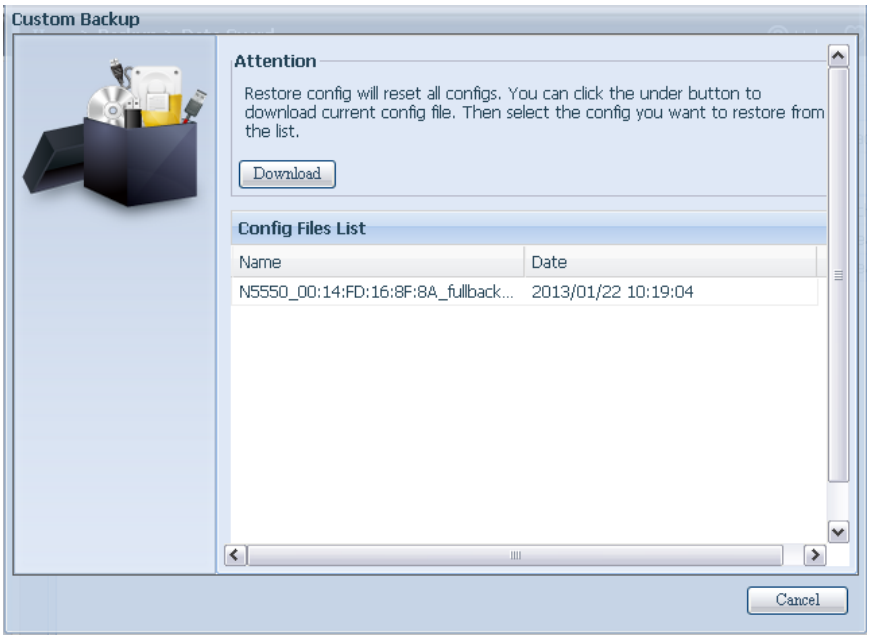
1. When adding a new backup task with "Full backup" or "Custom backup" and enabling the option "Backup NAS Config" as shows below, the source unit system configurations are then backed up to the designed path on the target system every time the task is executed.



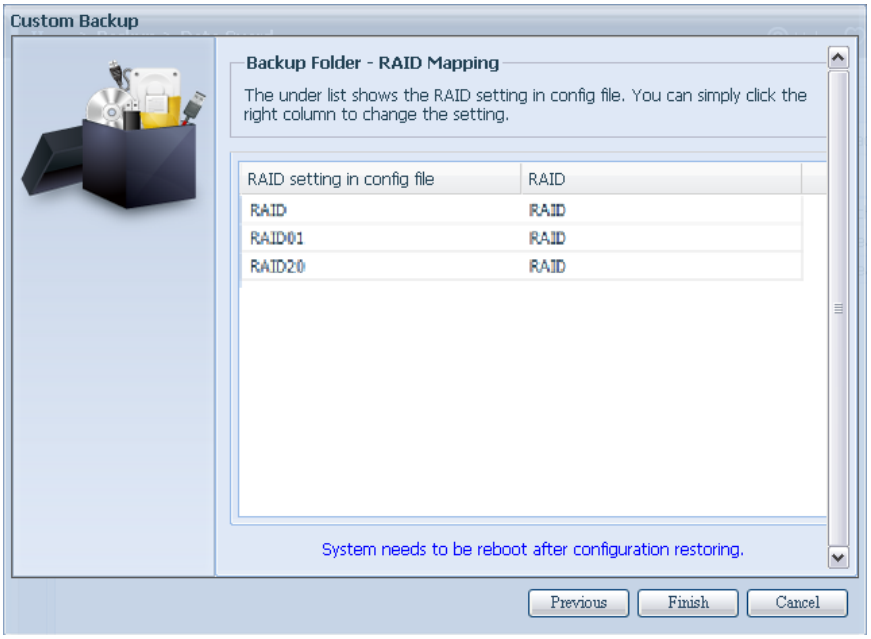
2. Click on "Restore NAS Configuration" and the screen shown below will appear. Input the target server's IP address where the system configuration has been backed up, and necessary authentication info. Confirm by doing a "Connection Test" to make sure the communication between the source and the target server works.



3. Click "Next" and a screen will appear as shown below. It has the listed available system configuration backup files. Select the one you want and click next. You also have the option to download the current system configuration before restoring from the backup file.


Custom Backup
Attention
Restore config will reset all configs. You can click the under button to download current config file. Then select the config you want to restore from the list.
Download
Config Files List
Name
Date
N5550_00:14:FD:16:8F:8A_fullback...
2013/01/22 10:19:04
Cancel

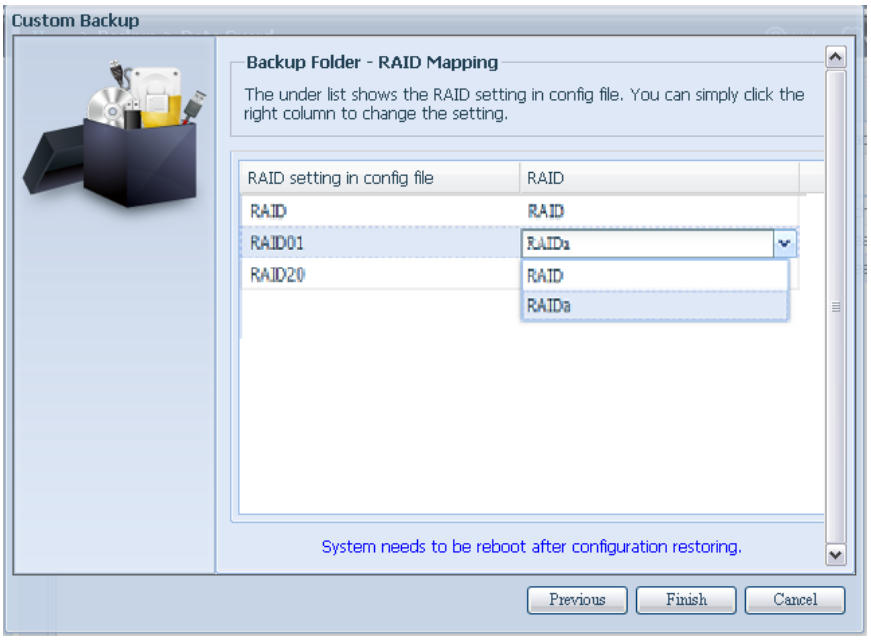
4. After clicking "Next", a screen will appear as shown below. Listed on the left hand side, you will see the configuration backup details which contain the 3 RAID volumes. On the right hand side, you will see a list of single "RAID" volume. You may roll back to previous page to recall the example we have taken.



5. The backup configuration has different numbers of RAID volume than the current system (3 vs 1). It can be kept as the RAID volume mapping arranged by the system, then carry on to click "Finish". This means that all 3 RAID volumes configuration such as share folder etc. will all restore to the current unit in the RAID volume "RAID".
6. In other circumstances, if the current unit contains 2 RAID volumes, then it can be chosen from the left hand side of system backup configuration RAID volume list which RAID volume to map to the current system.

   Let's see the following screen to make it clearer.

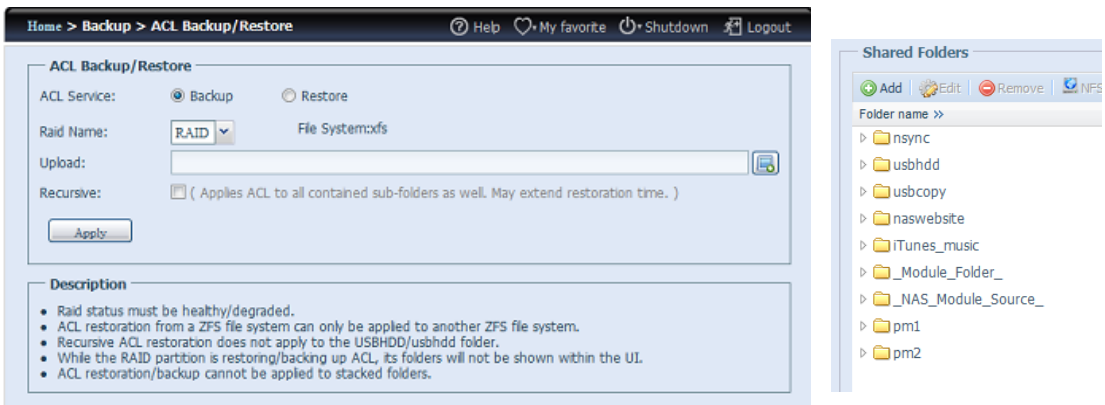
The current system has 2 RAID volumes, "RAID" and "RAIDa". Select the RAID volume from the backup configuration volume list which is going to be mapped to the RAID volume of the current system. Simply click on the right hand side of "RAIDa" and a drop down list will appear. Now you can choose which volume to map with. In this case the "RAID01" volume from the system backup configuration will be mapped to the volume "RAIDa" of the current unit. Once again, it means all the shares that were created in the volume "RAID01" will be restored to volume "RAIDa" of the current system.



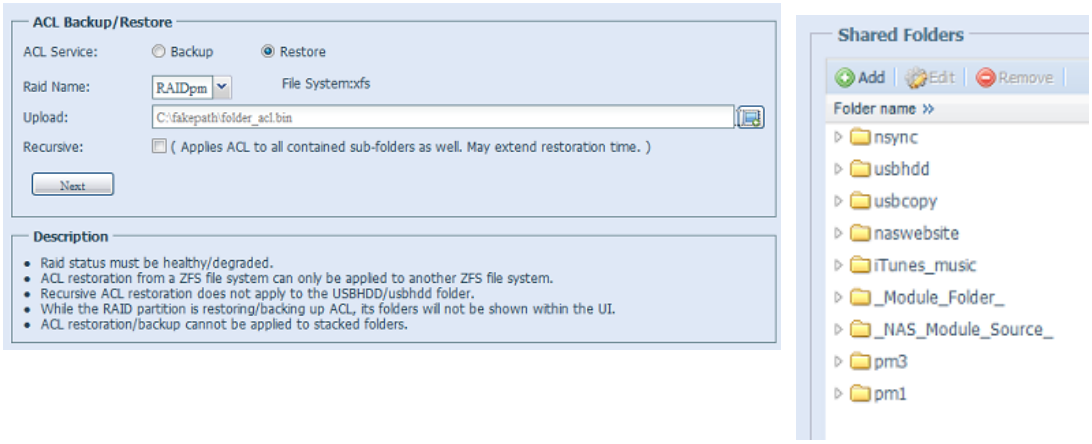
ACL Backup and Restore

The ACL backup and restore feature enables the system ACL (Access Control List) to be backed up on the RAID volume based to other location and restored if needed.

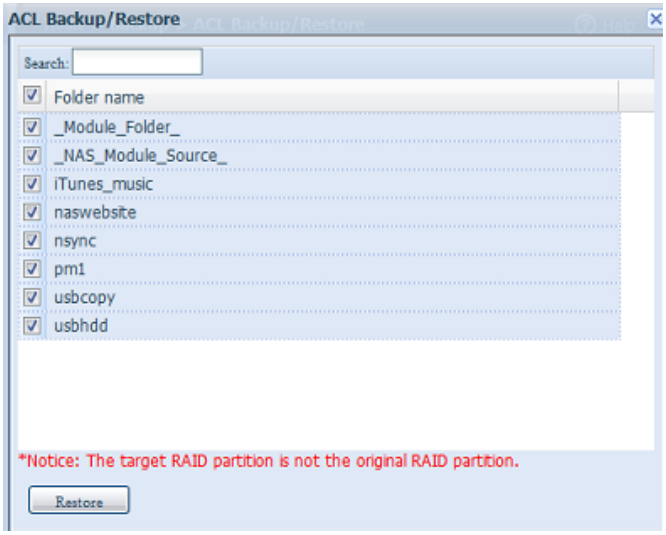
Let's look at the example bellow to see how it works.
We have one system with a RAID volume "RAID", select "Backup" to backup this RAID volume's ACL to other location. The current RAID volume "RAID" has share folder as listed on right hand screen shot.



For the ACL restore, it can be restored in the same system or used in another unit. For example, let's restore the ACL backup file to another unit. This unit has a RAID volume "RAIDpm" with share folders as listed on right hand screen shot.



After inputting the ACL backup file and clicking the "Next" button, the system will show another screen to list the matched folders in between the backup file and this RAID volume. Just select the desired folders for the ACL restore.

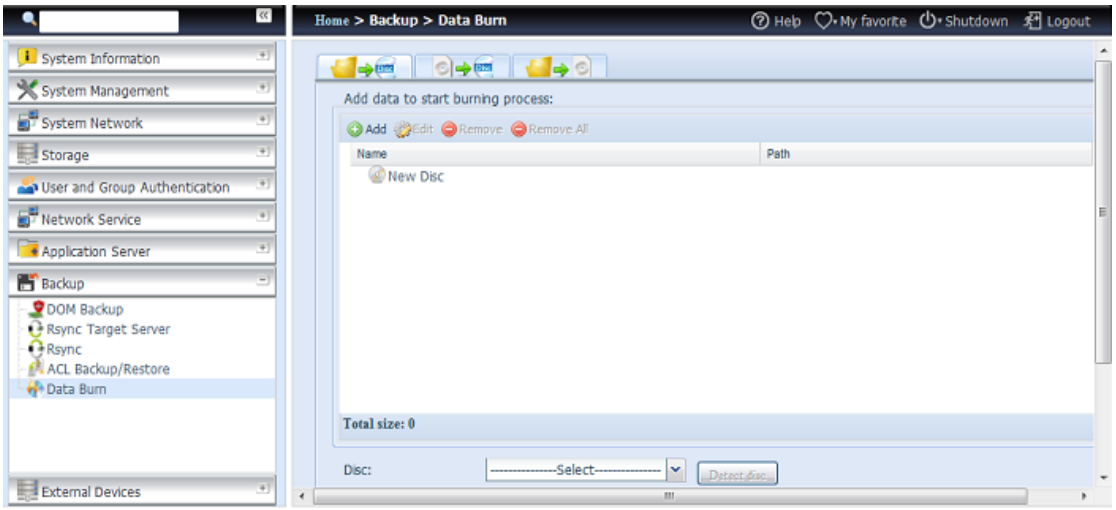


NOTE

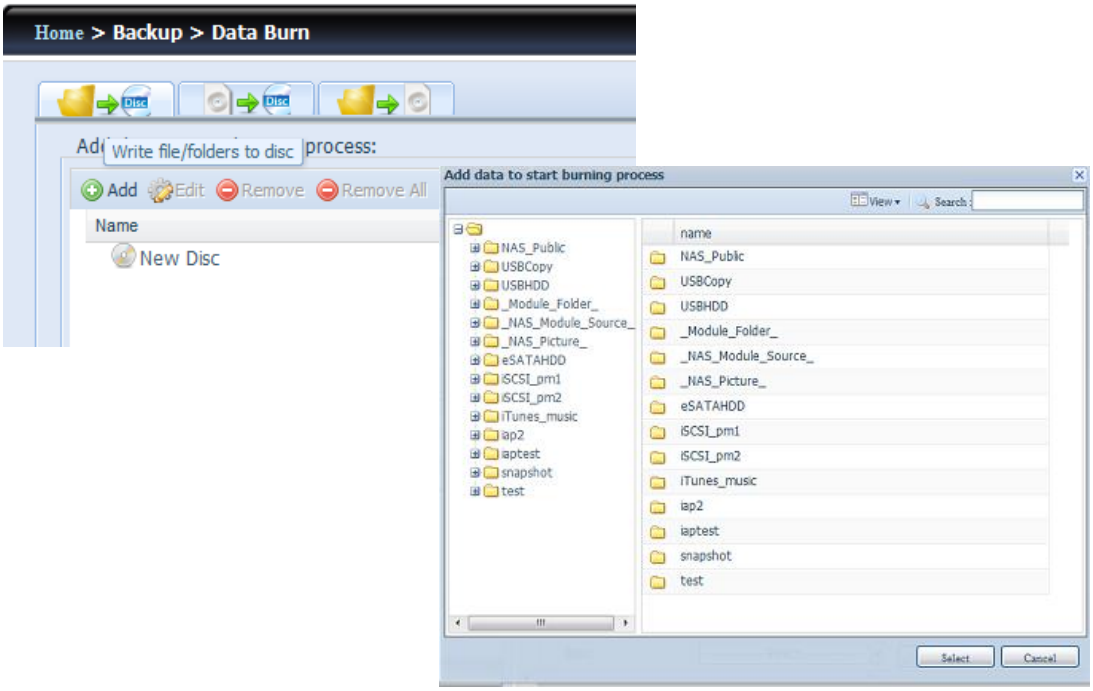
- The ACL backup will only back to share folder level; it does not apply to its sub-layer.
- The ACL backup/restore can be used among ext3/ext4/XFS file system. ZFS can only be used with other RAID volume with ZFS file system created.
- If recursive has been checked during the ACL restoration, it will apply to all of its sub-folders with the same permission.

Data Burn

The data burn is featured to support 3 different modes of data burning for files/folders to and from image file and physical optical disk.
The 3 different modes are "Write Files/folders to disc", "Write image to disk" and "Write files/folders to image".

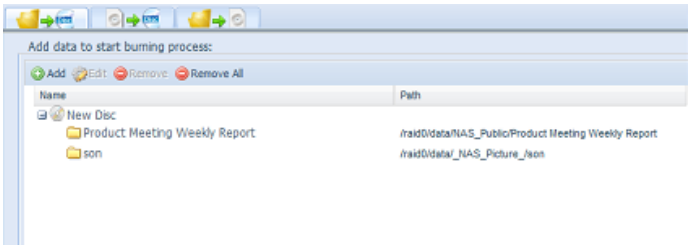


1. Write Files/folders to disc

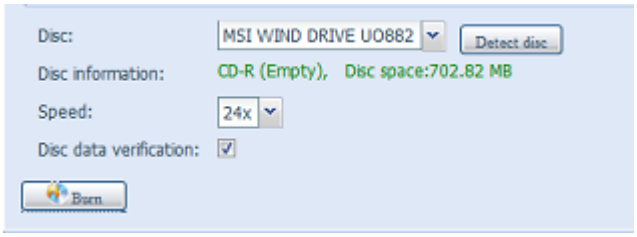


a. Click the Add button and the NAS share list appears.

b. Select files/folders which you would like to burn. All of the selected folders/files will be seen under the disc label name "New Disc". The disc label name can be changed by clicking on it and press "Edit" from menu bar. The selected folders/files also can be removed by clicking on them and then pressing "remove" or "remove all" for all selected items.

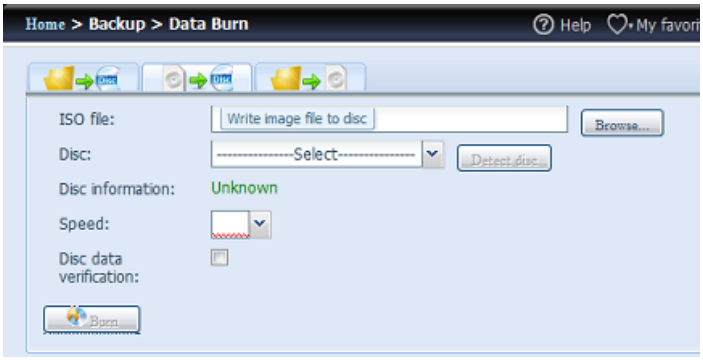


c. Select from the installed USB or SATA(for N6850/N8850/N10850) burning devices. Please click the "detect disc" button to check the status once the disc is inserted.

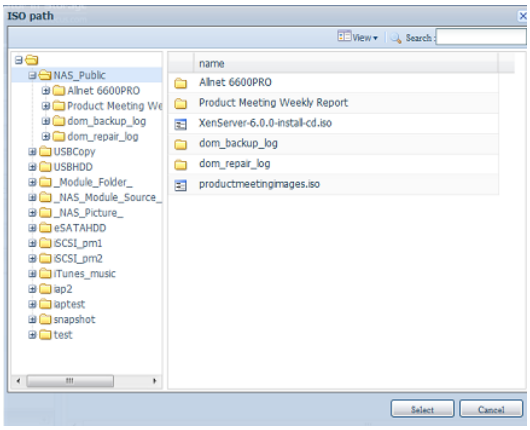


d. Select the burning speed from the drop down list.
e. Select whether disc data verification is required or not.
f. Click "Burn" to start disc burning.

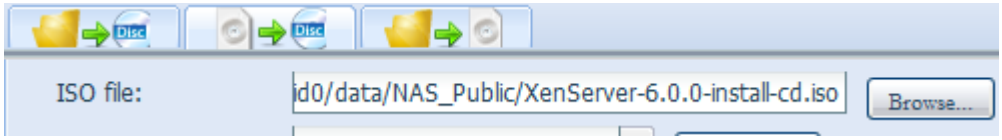
2. Write image file to disc



a. Click "Browser" and the NAS share list will appear to locate the desired image file to burn.

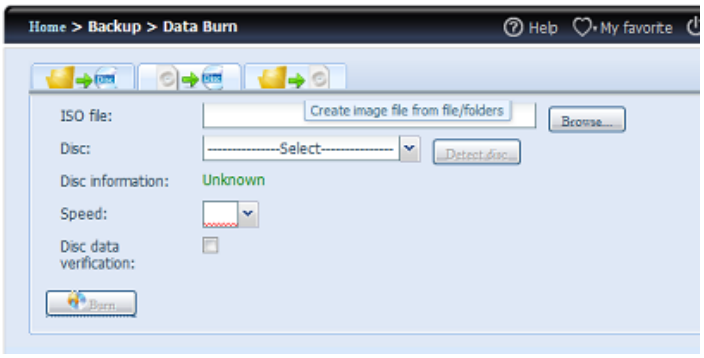


b. Select the ISO file.

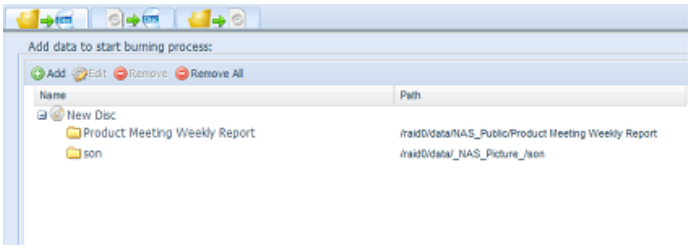


c. Select from the installed USB or SATA(for N6850/N8850/N10850) burning devices. Please click the "detect disc" button to check the status once the disc is inserted.
d. Select the burning speed from the drop down list.
e. Select whether disc data verification is required or not.
f. Click "Burn" to start disc burning.

3. Create image file from files/folders



a. Click the Add button and the NAS share list will appear.
b. Select the files/folders which you would like to burn. All of the selected folders/files will appear under the disc label name "New Disc". The disc label name can be changed by clicking on it and pressing "Edit" from the menu bar. The selected folders/files also can be removed by clicking on them and pressing "remove" or "remove all" for all the selected items.



c. Input the path where the ISO file is going to be stored, you can press the "Browse" button to have the share list appear.
d. Input the ISO file name for burned image file.
e. Click "Burn" to start the ISO file burning.

NOTE

- The data burn does not support rewriteable media if it has been burned with left space. On the other hand, the used rewriteable media will be erased first then carry on with burning.

Thecus Backup Utility

The Thecus Backup Utility is on your Installation CD. When you click on the CD, the Backup Utility will be installed under **Program Groups** > **Thecus** > **Thecus Backup Utility**. If it is not installed, you can copy the file (**Thecus Backup Utility.exe**) to a convenient location on your hard disk and double click to execute it.

NOTE

If you can not find Thecus Backup Utility on your CD, please download it from the Thecus website (http://www.thecus.com).

When you execute this utility for the first time, it will ask you to create a DB file. Click ***Yes***.

1. Click ***Add*** to create a Backup task. The **Add New Task** dialog box will appear.

Add New Task	
Item	**Description**
Task	Specifies a name for the current task.
Source	Click to specify the source folder/file location.
Incremental	Click to specify whether the backup will be incremental. If unchecked, the backup will be a full backup.
Destination	Click to specify the destination folder/file location.
Excluded extensions	Files with these file name extensions will be skipped and not backed up to the destination.
Comments	If you wish, enter a comment here for your records.

2. To schedule the task to run at regular intervals, click on the ***Schedule*** icon for that task. You can schedule the task to run **Monthly** or **Weekly**.

3. To check the log for that task, click on the ***Log*** icon for that task.

NOTE

Thecus Backup Utility also supports MAC OS X. Just copy the Thecus Backup Utility.dmg to your MAC OS X machine and double click to execute it.

Windows XP Data Backup

If you use Windows XP Professional, you can also use the Windows Backup Utility (Ntbackup.exe) to back up your files.

If you use Windows XP Home Edition, follow these steps to install the utility:

1. Insert the Windows XP CD into a drive and double-click the ***CD*** icon in **My Computer**.

2. When the Welcome to Microsoft Windows XP screen appears, click ***Perform Additional Tasks***.

3. Click ***Browse this CD***.

4. In Windows Explorer, navigate to ***ValueAdd*** > ***Msft*** > ***Ntbackup***.

5. Double-click ***Ntbackup.msi*** to install the backup utility.

Once installed, you can use the Windows Backup Utility by following the steps below:

1. Click ***Start***, and point to ***All Programs*** > ***Accessories*** > ***System Tools*** > ***Backup*** to start the wizard.

2. Click ***Next*** to skip past the opening page. Choose **Backup files and settings** from the second page, and then click ***Next***.

3. Select which option you want to back up.

4. Click ***Next*** and in the Backup Type, Destination, and Name page, specify a backup location using the ***Browse*** button.

5. Find and select the drive that specifies your Thecus IP storage as your backup destination and click ***Next***.

6. Click ***Next*** to display the wizard's final page and click ***Finish*** to start backing up.

Apple OS X Backup Utilities

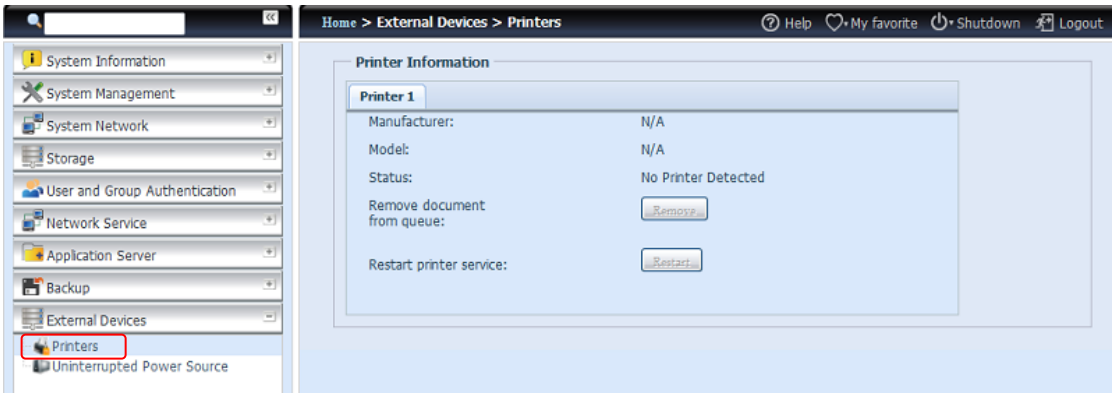
Mac OS X does not include any backup software. However, there are a number of backup solutions available for the Mac OS X, including: iBackup, Psyncx, iMSafe, Rsyncx, Folder Synchronizer X, Tri-BACKUP, Impression, Intego Personal Backup, SilverKeeper, and Apple's dotMac Backup utility to name just a few. To find even more freeware and shareware backup utilities to choose from, go to VersionTracker or MacUpdate and search on "backup".

External Devices

The Thecus IP storage supports printer server and UPS via USB interface. The integrated Print Server allows you to share a single USB printer with all users on the network. For the UPS, Thecus IP storage support via USB, Series and Network interface. The following section shows you how.

Printers

From the **External Devices** menu, choose the ***Printer*** item, and the **Printer Information** screen appears. This screen provides the following information about the USB printer connected to the USB port.



Printer Information	
Item	**Description**
Manufacturer	Displays the name of the USB printer manufacturer.
Model	Displays the model of the USB printer.
Status	Displays the status of the USB printer.
Remove document from Queue	Click to remove all documents from printer queue
Restart Printer service	Click to restart printer service

If a corrupt print job is sent to a printer, printing may suddenly fail. If your print jobs seem to be locked up, pressing the ***Remove All Documents*** button to clear the print queue may resolve the issue.

You can configure Thecus IP storage to act as a printer server. That way, all PCs connected to the network can utilize the same printer.

Windows XP SP2

To set up the Printer Server in Windows XP SP2, follow the steps below:

1. Connect the USB printer to one of the USB ports (preferably the rear USB ports; front USB ports can be used for external HDD enclosures).
2. Go to ***Start*** > ***Printers and Faxes***.
3. Click on **File** > **Add Printer**.
4. The **Add Printer Wizard** appears on your screen. Click ***Next***.
5. Select the "***A network printer, or a printer attached to another computer***" option.
6. Select "***Connect to a printer on the Internet or on a home or office network***", and enter "**`http://Thecus IP storage IP_ADDRESS:631/printers/usb-printer`**" into the URL field.
7. Your Windows system will ask you to install drivers for your printer. Select the correct driver for your printer.
8. Your Windows system will ask you if you want to set this printer as "Default Printer". Select ***Yes*** and all your print jobs will be submitted to this printer by default. Click ***Next***.
9. Click ***Finish***.

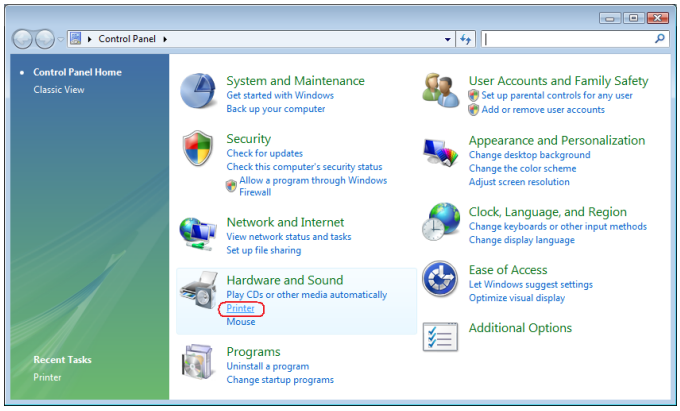
NOTE

- Note that if a multi-function (all-in-one) printer is attached to the Thecus IP Storage, usually only the printing and fax functions will work. Other features, such as scanning, will probably not function.

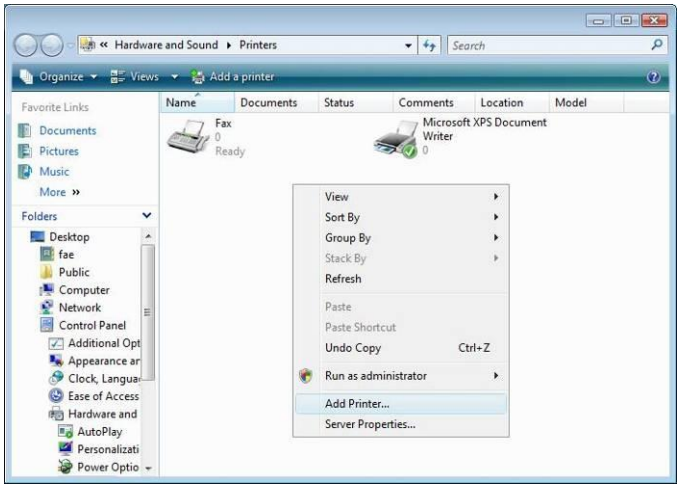
Windows Vista

To set up the Printer Server in Windows Vista, follow the steps below:

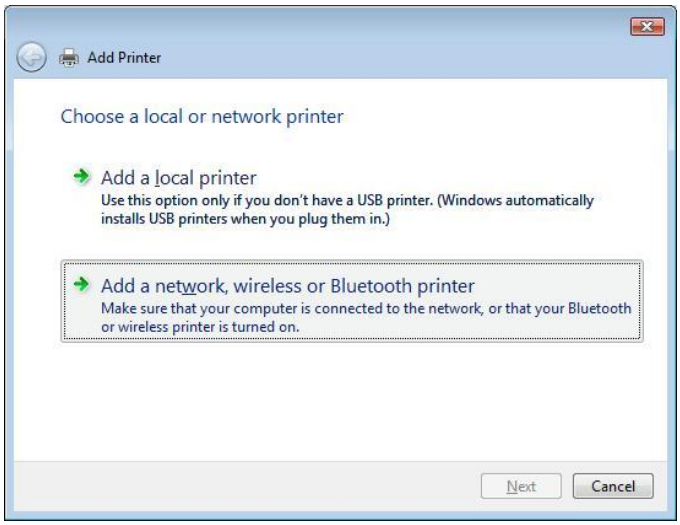
1. Open ***Printer Folder*** from the **Control Panel**.



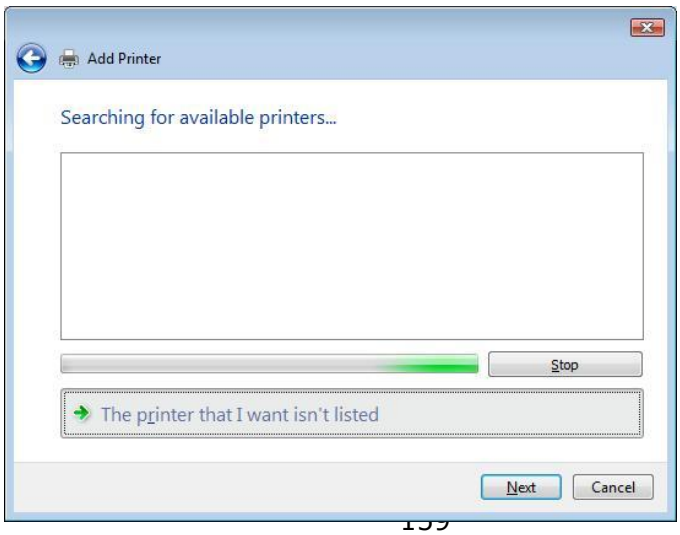
2. Click the right mouse button in anywhere on the **Printers** folder and then select ***Add Printer***.



3. Select ***Add a network, wireless or Bluetooth printer***.

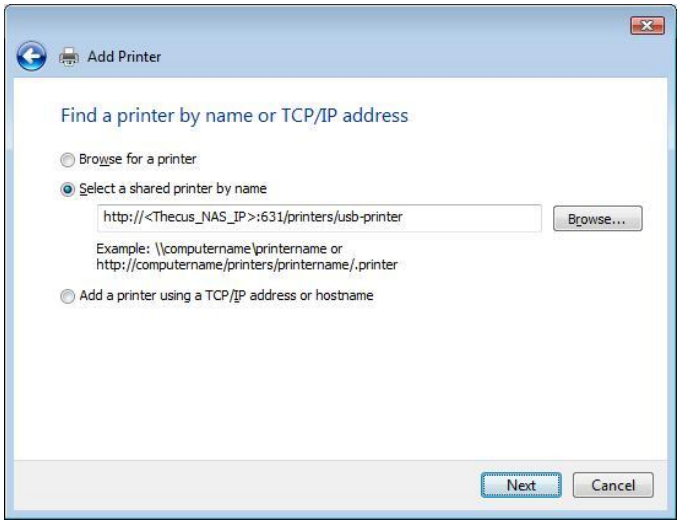

Add Printer
Choose a local or network printer
Add a local printer
Use this option only if you don't have a USB printer. (Windows automatically installs USB printers when you plug them in.)
Add a network, wireless or Bluetooth printer
Make sure that your computer is connected to the network, or that your Bluetooth or wireless printer is turned on.
Next
Cancel

4. Select ***The printer that I want isn't listed***.



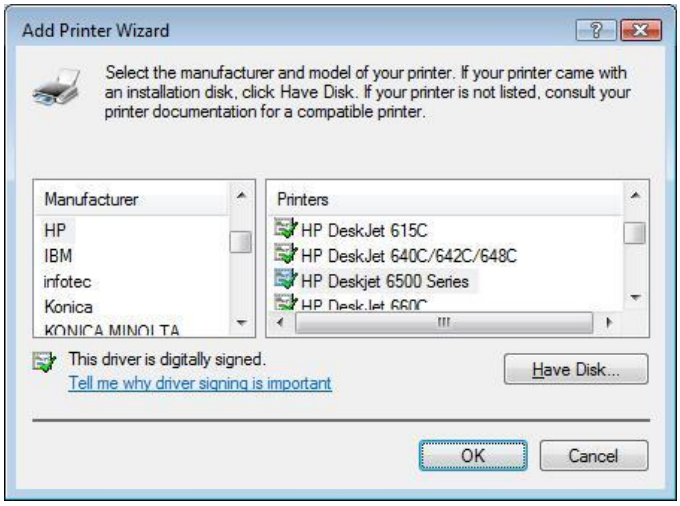
You can press ***The printer that I want isn't listed*** to go into next page without waiting for **Searching for available printers** to finish.

5. Click ***Select a shared printer by name***.

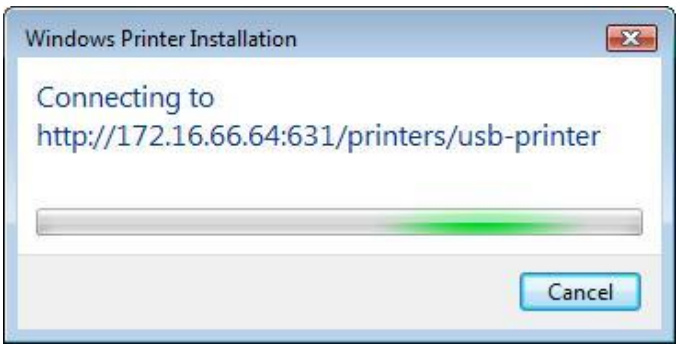


Type `http://<Thecus_NAS>:631/printers/usb-printer` in the box, where `<Thecus_NAS_IP>` is the IP address of Thecus IP storage. Click ***Next***.

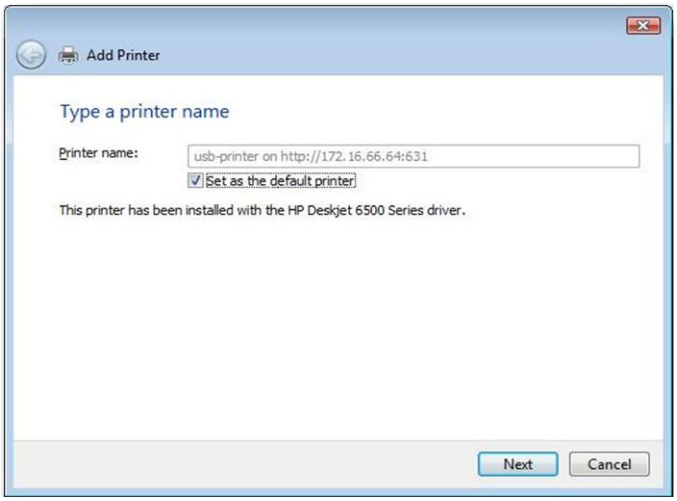
6. Select or install a printer and then press ***OK***.


Add Printer Wizard
Select the manufacturer and model of your printer. If your printer came with an installation disk, click Have Disk. If your printer is not listed, consult your printer documentation for a compatible printer.
Manufacturer
HP
IBM
infotec
Konica
Printers
HP DeskJet 615C
HP DeskJet 640C/642C/648C
HP Deskjet 6500 Series
This driver is digitally signed.
Tell me why driver signing is important
Have Disk...
OK
Cancel

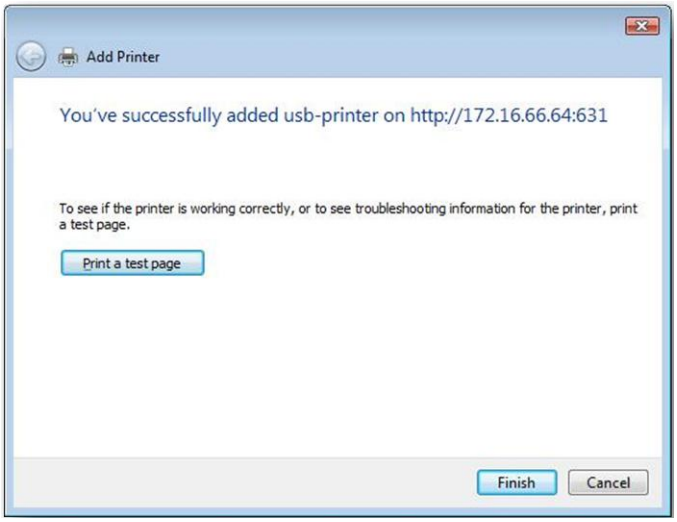
7. Windows will attempt to connect to the printer.



8. You can choose to set this printer as the default printer by checking the ***Set as the default printer*** box. Click ***Next*** to continue.

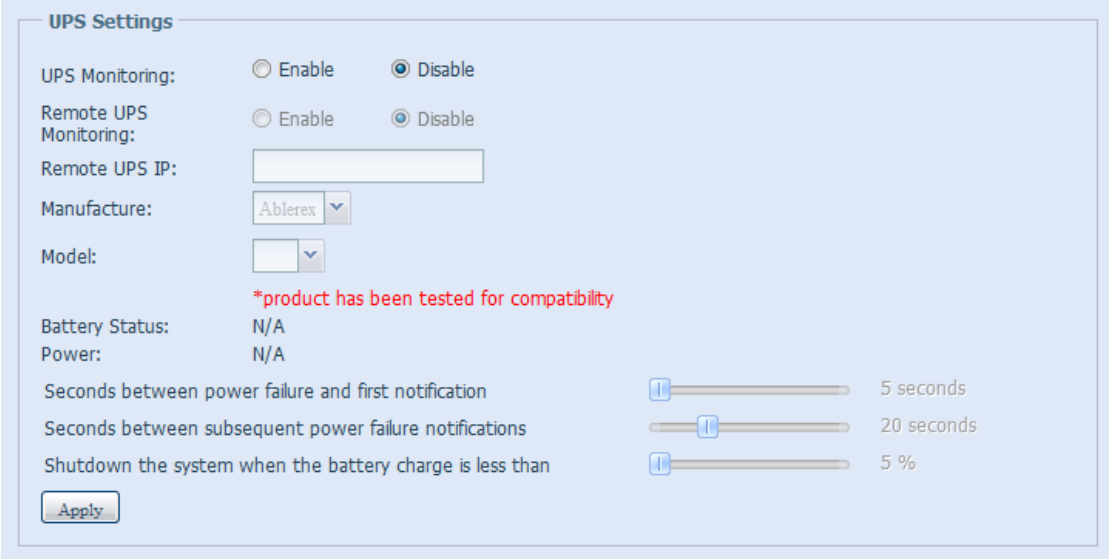


9. Done! Click ***Finish***.


Add Printer
You've successfully added usb-printer on http://172.16.66.64:631
To see if the printer is working correctly, or to see troubleshooting information for the printer, print a test page.
Print a test page
Finish
Cancel

Uninterrupted Power Source

From the **External Devices** menu, choose the ***Uninterrupted Power Source*** item and the **UPS Setting** screen appears. Make any changes you wish, and press ***Apply*** to confirm changes.



See the following table for a detailed description of each item.

UPS Setting	
Item	**Description**
UPS Monitoring	Enable or disable UPS monitoring.
Remote UPS Monitoring	Enable or disable Remote UPS monitoring.
Remote UPS IP	Input the IP address of the NAS that the UPS device is connected to via USB or RS232.Input the IP address of your network UPS.
Manufacturer	Choose the UPS manufacturer from the dropdowns.
Model	Choose the UPS model number from the dropdowns.
Battery Status	Current status of the UPS battery
Power	Current status of the power being supplied to the UPS
Seconds between power failure and first notification	Delay between power failure and first notification in seconds.
Seconds between subsequent power failure notifications	Delay between subsequent notifications in seconds.
Shutdown the system when the battery charge is less than	Amount of UPS battery remaining before system should auto-shutdown.
Apply	Press ***Apply*** to save your changes.

Chapter 5: Tips and Tricks

USB and eSATA Storage Expansion

The Thecus IP storage supports external USB hard disks through its USB ports. Once a USB hard disk is successfully mounted, the entire volume will be linked automatically to the default USB HDD folder. The Thecus IP storage supports USB external storage devices. All file names on the USB disk volume are case sensitive.

The Thecus IP storage also supports eSATA hard disks with its eSATA port.

Before attaching an eSATA or USB disk drive to Thecus IP storage, you have to partition and format it on a desktop computer or a notebook first. The attached device will be located at `\\192.168.1.100\usbhdd\sd(x)1` where `192.168.1.100` means the IP address of Thecus IP storage and `sd(x)1` stands for the first partition on the eSATA or USB disk drive.

Remote Administration

You can set up your Thecus IP storage for remote administration. With remote administration, you can access your Thecus IP storage over the Internet, even if your Thecus IP storage is behind a router. This is especially useful if you are traveling and suddenly need a file from your Thecus IP storage.

Setting up remote administration is a three-part process, and will require the following equipment:

- Thecus IP storage device
- Cable / DSL Router with Dynamic DNS support
- Home PC
- Internet Connection

NOTE

Router setup will differ slightly depending on router used. For this example, we will use the Asus WL500g because it has support for Dynamic DNS. Contact your router hardware vendor for setup help.

Part I - Setup a DynDNS Account

1. Go to `http://www.dyndns.org` from your home PC.
2. Click on the ***Sign Up Now*** link.
3. Check the Check boxes, select a user name (i.e.: N12000), enter your email address (i.e.: xxx@example.com), check ***Enable Wildcard***, and create a password (i.e.: xxxx).
4. Wait for an email from www.dyndns.org.
5. Open the email and click on the link to activate your account

Part II - Enable DDNS on the Router

1. Go to the router setup screen and select ***IP Config*** > ***Miscellaneous DDNS Setting*** from your Home PC.
2. Click on ***Yes*** for **Enable the DDNS Client?**
3. Select **`www.dyndns.org`**.
4. Go to router setup screen, and enter the following information:
    a. User Name or E-mail Address: **xxx@example.com**
    b. Password or DDNS Key: **xxxx**
    c. Host Name: **`www.N12000.dyndns.org`**
    d. Enable wildcard? Select ***Yes***
    e. Update Manually: Click ***Update***

Part III - Setting up Virtual Servers (HTTPS)

1. Navigate to ***NAT Setting*** > ***Virtual Server***.
2. For **Enable Virtual Server?**, select ***Yes***
3. Setup the HTTPS Server
    a. **Well-Known Applications**: Select **User Defined**
    b. **Local IP**: Enter **`192.168.1.100`**
    c. **Port Range**: **`443`** (the default HTTPS port setting on the Thecus IP storage)
    d. **Protocol**: select **TCP**
    e. Click ***Add***.
    f. Click ***Apply***.
4. Test the HTTPS connection from another computer on the Internet
    a. From a remote computer, open your browser and enter **`https://www.N12000.dyndns.org`**
    b. You should see the login page of Thecus IP storage.

Firewall Software Configuration

If you are using a software firewall (i.e. Norton Internet Security) and are having trouble connecting to Thecus IP storage, you can try the following steps:

1. Double click the **NIS** icon on system tray, and then configure the **Personal Firewall**.

2. On the **Programs** page, find the **SetupWizard.exe** and change its permission to "Permit All". If it's not in the program list, use the **Add** or **Program Scan** buttons to find it.

3. On the **Networking** page, manually add Thecus IP storage IP address (i.e. `192.168.1.100`) to the **Trusted** list.

Replacing Damaged Hard Drives

If you are using RAID 1, RAID 5, RAID 6, RAID 50 or RAID 60 you can easily replace a damaged hard drive in the Thecus IP storage while keeping your data secure with the system's automatic data recovery.

Hard Drive Damage

When a hard drive is damaged and data in the RAID volume is corrupted, the system OLED will display a warning message and the system will beep.

Replacing a Hard Drive

To replace a hard disk drive in the Thecus IP storage:

1. Remove the tray with the damaged hard disk.
2. Unscrew the damaged hard disk and remove it from the tray.
3. Slide a new hard disk into the tray and fasten the screws.
4. Insert the hard disk tray back into the Thecus IP storage until it snaps into place. You can also lock it with a key if desired.
5. The LED will blink green when the HDD is accessed.

RAID Auto-Rebuild

When using RAID 1, 5, 6, 10, 50 or 60 on the Thecus IP storage, you can use the auto-rebuild function when an error is detected.

1. When a hard disk fails the system beeps and/or an email notification is sent to the specified receivers.
2. Check the OLED to see which disk has failed.
3. Follow the steps mentioned above to replace the failed hard disk.
4. The system automatically recognizes the new hard disk and starts the auto-rebuild sequence to resume its status before the hard disk crash.

Chapter 6: Troubleshooting

Forgot My Network IP Address

If you forget your network IP address and have no physical access to the system, you can find out the IP address by either looking directly onto the Thecus IP storage OLED panel, or by using the setup wizard to retrieve the IP of your Thecus IP storage.

1. Start the Setup Wizard, and it will automatically detect all Thecus IP storage products on your network.

2. You should be able to find the IP address of the Thecus IP storage which you have forgotten in the **Device Discovery** screen.

Can't Map a Network Drive in Windows XP

You may have problems mapping a network drive under the following conditions:

1. The network folder is currently mapped using a different user name and password. To connect using a different user name and password, first disconnect any existing mappings to this network share.

2. The mapped network drive could not be created because the following error has occurred: **Multiple connections to a server or shared resource by the same user, using more than one user name, are not allowed.** Disconnect all previous connections to the server or shared resource and try again.

To check out existing network connections, type `net use` under the DOS prompt. You may refer the URL below for more network mapping information.

http://esupport.thecus.com/support/index.php?_m=downloads&_a=viewdownload&downloaditemid=57&nav=0

Restoring Factory Defaults

From the **System** menu, choose the ***Factory Default*** item and **the Reset to Factory Default** screen appears. Press ***Apply*** to reset Thecus IP storage factory default settings.

WARNING

Resetting to factory defaults will not erase the data stored in the hard disks, but WILL revert all the settings to the factory default values.

Problems with Time and Date Settings

The administrator is able to select an NTP Server to keep Thecus IP storage time synchronized. However, if Thecus IP storage cannot access the Internet, you may encounter a problem when setting the Time and Time Zone. If this happens:

1. Login to the Web Administration Interface.
2. Navigate to **System Management>*Time***.
3. Under **NTP Server**, select ***No***.
4. Set the **Date**, **Time**, and **Time Zone**.
5. Click ***Apply***.

In addition, if the Thecus IP storage is able to access the Internet and you want to keep the NTP Server clock.isc.org by default, please make sure the DNS Server is correctly entered, thereby allowing the NTP Server name to correctly resolve. (See **System *Network*** > ***WAN/LAN1*** > ***DNS Server***)

Dual DOM Supports for Dual Protection (N12000 series/N16000 series/N8900 series only)

The most advance and useful feature on the Thecus IP storage (depend on models) is the implemented Dual DOM. Under normal circumstances, there is no need to have this feature involved. But some unpredictable problems like power cut or human error can occur by accident, especially during system booting stage; the Dual Dom will become the best feature to prevent system down time.
Practically while it happened, system will try to recover the DOM 1 from DOM 2 first. If it is unachievable then the system can boot from DOM 2. And all of these procedures can be operated through the OLED.

NOTE

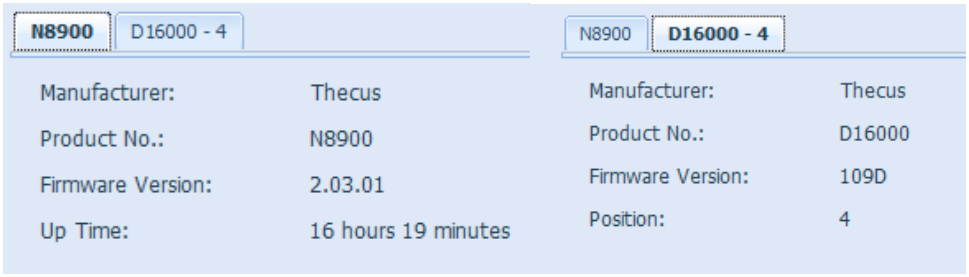
The DOM1 in Dual DOM is by default the master DOM and FW updates will only apply to DOM1. DOM2 is 'Read only".
If anything happened and the DOM1 is recovered from DOM2, the FW version will be the one of the DOM2. Therefore, it may need to be upgraded to the version of DOM1.
If DOM1 can not be recovered from DOM2, the system will boot up from DOM2. The original configuration of DOM1 may need to be setup again with DOM2 operations.

Chapter 7: Updates for FW v2.03.01

Changes for FW v2.03.01
- Added JBOD device info to **General** in the **System Information** category
- Modifed the **Status** layout in the **System Information** category
- Added **Hardware Information** in the **System Information** category
- Modified **Disk Information** layout and added support for JBOD device
- Added JBOD device to join **RAID Management**
- Added cloud backup **Amazon S3** support
- Added **Volume Expansion Management** in the Storage category

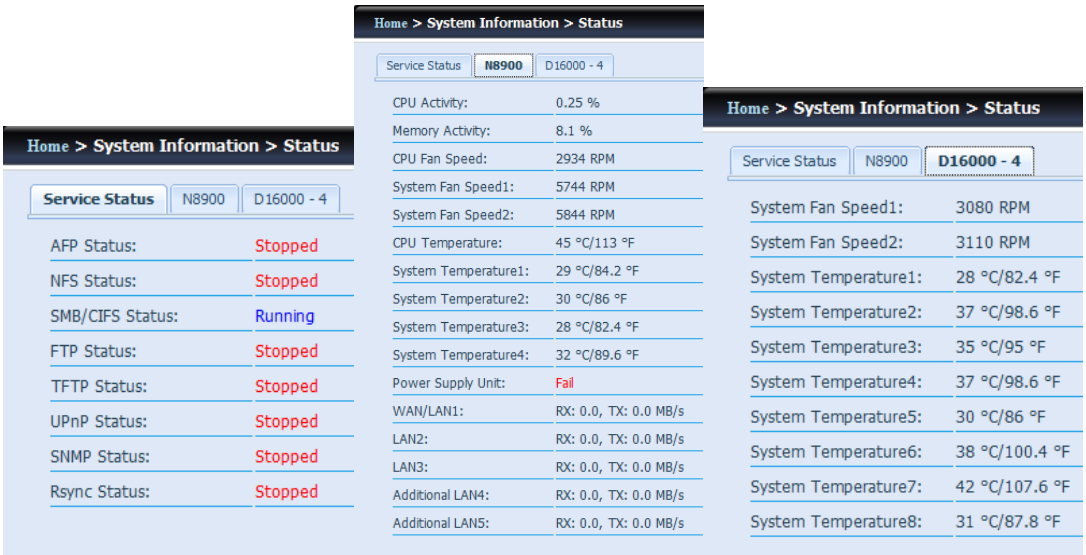
General

The Thecus N8900/N12000/N16000 series are supporting the addition of the JBOD device Thecus D16000 to expand storage capacity. From **General** in **System Information,** JBOD device info will be displayed if applicable.



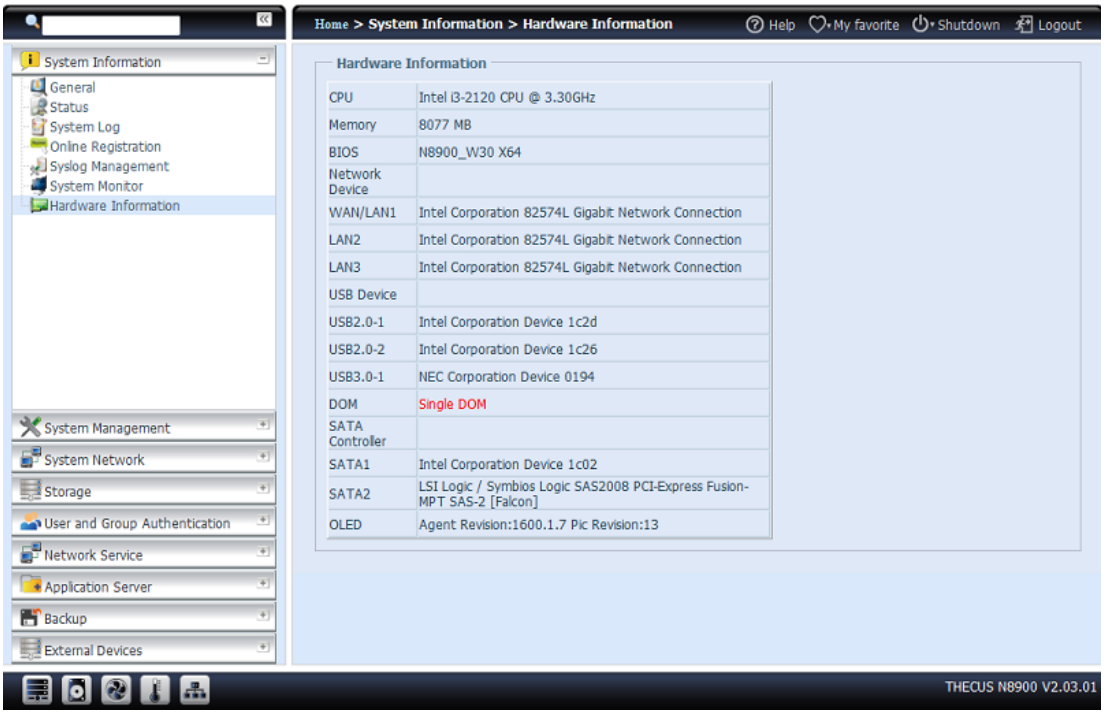
Status

From the **System Information** menu, choose the ***Status*** item, **System Service Status** and HW **Status** screens appear. These screens provide basic system and service status information.


Home > System Information > Status
Service Status
N8900
D16000 - 4
AFP Status: Stopped
NFS Status: Stopped
SMB/CIFS Status: Running
FTP Status: Stopped
TFTP Status: Stopped
UPnP Status: Stopped
SNMP Status: Stopped
Rsync Status: Stopped
Home > System Information > Status
Service Status
N8900
D16000 - 4
CPU Activity: 0.25 %
Memory Activity: 8.1 %
CPU Fan Speed: 2934 RPM
System Fan Speed1: 5744 RPM
System Fan Speed2: 5844 RPM
CPU Temperature: 45 °C/113 °F
System Temperature1: 29 °C/84.2 °F
System Temperature2: 30 °C/86 °F
System Temperature3: 28 °C/82.4 °F
System Temperature4: 32 °C/89.6 °F
Power Supply Unit: Fail
WAN/LAN1: RX: 0.0, TX: 0.0 MB/s
LAN2: RX: 0.0, TX: 0.0 MB/s
LAN3: RX: 0.0, TX: 0.0 MB/s
Additional LAN4: RX: 0.0, TX: 0.0 MB/s
Additional LAN5: RX: 0.0, TX: 0.0 MB/s
Home > System Information > Status
Service Status
N8900
D16000 - 4
System Fan Speed1: 3080 RPM
System Fan Speed2: 3110 RPM
System Temperature1: 28 °C/82.4 °F
System Temperature2: 37 °C/98.6 °F
System Temperature3: 35 °C/95 °F
System Temperature4: 37 °C/98.6 °F
System Temperature5: 30 °C/86 °F
System Temperature6: 38 °C/100.4 °F
System Temperature7: 42 °C/107.6 °F
System Temperature8: 31 °C/87.8 °F

Added Hardware Information

From the ***System Information*** *category*, choose the ***Hardware Information*** item and the system will display the related HW details for the associated model. Below is an example of the information for a Thecus N8900.

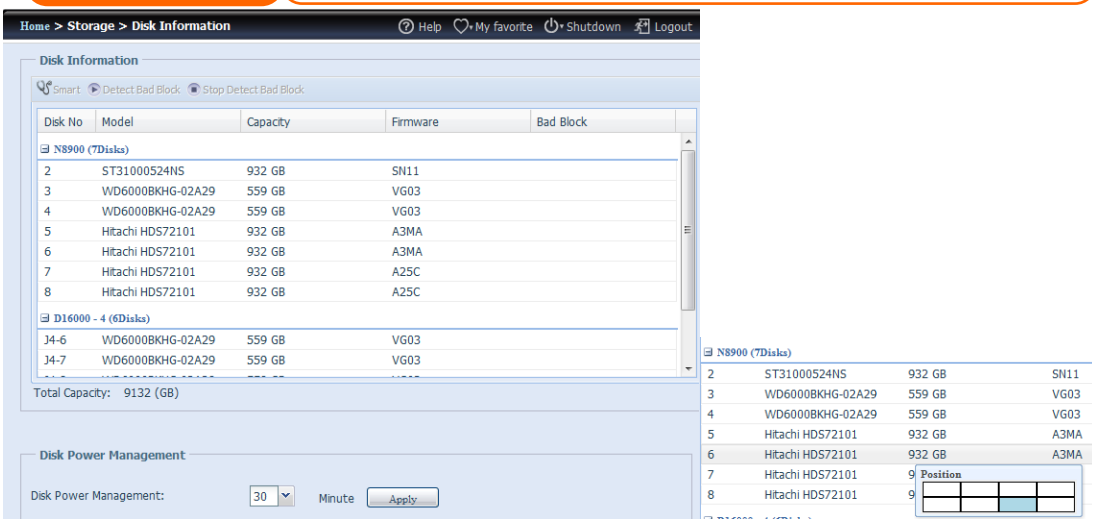


Disk Information

From the **Storage** menu, choose the ***Disk Information*** item and the **Disk Information** screen appears. From here, you can see various installed hard disks. The disk slot position will appear if the mouse is moved over the installed disk.

NOTE

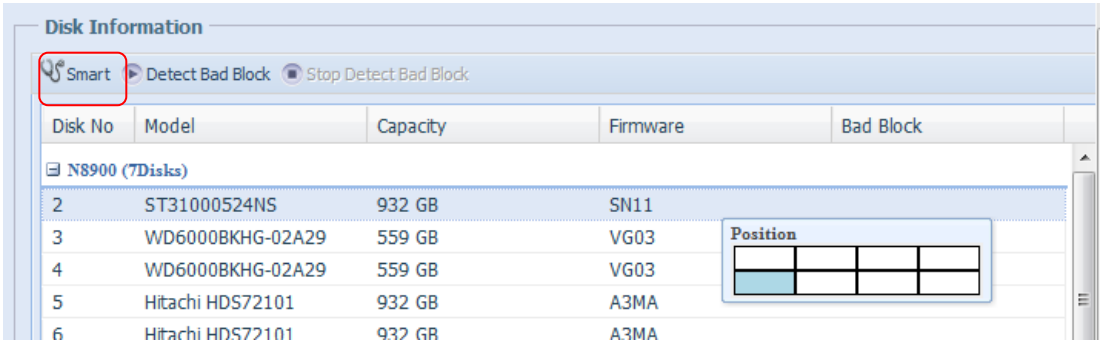
- The screen shot below is just an example from a Thecus IP Storage. The disk slots number can range from 8, 12 to 16 slots depending on the model of Thecus IP storage. Also it will list the disk info of JBOD devices if applicable



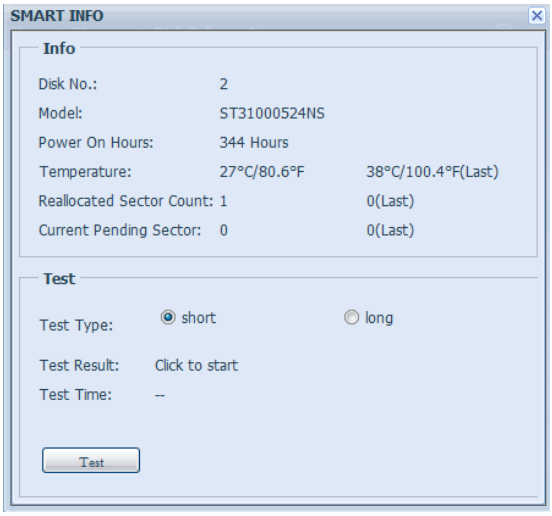
Disks Information	
Item	**Description**
Disk No.	Indicates disk location.
Capacity	Shows the SATA hard disk capacity.
Model	Displays the SATA hard disk model name.
Firmware	Shows the SATA hard disk firmware version.
Bad Block scan	Yes to start scan Bad Block.

S.M.A.R.T. Information

On the **Disk Information** screen, select a disk then click on "Smart" to list the **S.M.A.R.T.** info of the associated disk.



You may also perform a disk SMART test (doesn't apply to SAS HDD); simply click "Test" to start the SMART test. The result is only for reference and the system will not take any action from its results.



S.M.A.R.T. Information	
Item	**Description**
Tray Number	Tray the hard disk is installed in.
Model	Model name of the installed hard disk.
Power ON Hours	Count of hours in power-on state. The raw value of this attribute shows total count of hours (or minutes, or seconds, depending on manufacturer) in power-on state.
Temperature Celsius	The current temperature of the hard disk in degrees Celsius.
Reallocated Sector Count	Count of reallocated sectors. When the hard drive finds a read/write/verification error, it marks this sector as "reallocated"

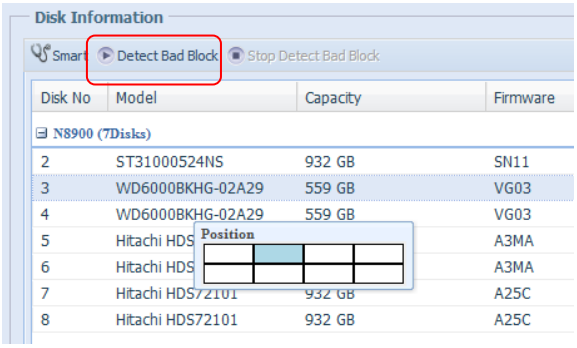
	and transfers data to a special reserved area (spare area). This process is also known as remapping and "reallocated" sectors are called remaps. This is why, on a modern hard disks, you cannot see "bad blocks" while testing the surface - all bad blocks are hidden in reallocated sectors. However, the more sectors that are reallocated, the more a decrease (up to 10% or more) can be noticed in disk read/write speeds.
Current Pending Sector	Current count of unstable sectors (waiting for remapping). The raw value of this attribute indicates the total number of sectors waiting for remapping. Later, when some of these sectors are read successfully, the value is decreased. If errors still occur when reading sectors, the hard drive will try to restore the data, transfer it to the reserved disk area (spare area), and mark this sector as remapped. If this attribute value remains at zero, it indicates that the quality of the corresponding surface area is low.
Test Type	Set short or long time to test.
Test Result	Result of the test.
Test Time	Total time of the test.

NOTE

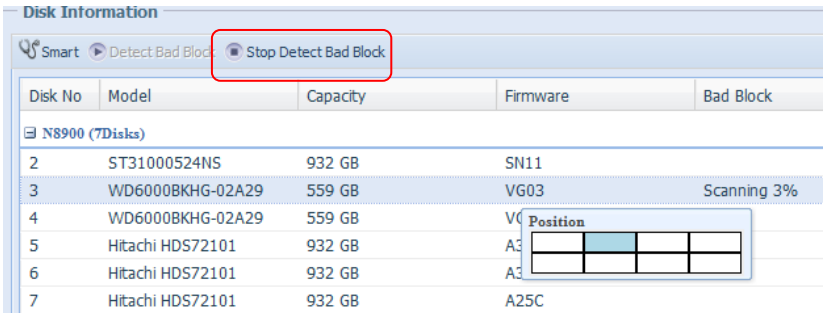
If the Reallocated Sector Count > 32 or the Current Pending Sector of a hard disk drive > 0 , the status of the disk will show "Warning". This warning is only used to alert the system administrator that there are bad sectors on the disk, and they should replace those disks as soon as possible.

Bad Block Scan

On the **Disk Information** screen, select a disk then click on "Detect Bad Block" to perform bad block scan of the associated disk. The result is only for reference and the system will not take any action from its results.

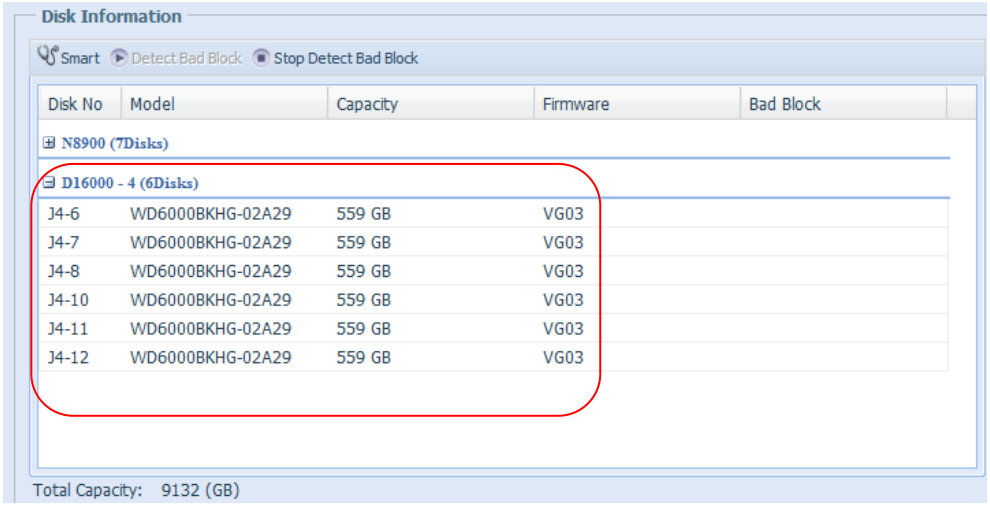


The bad block scan can be terminated by clicking on "Stop Detect Bad Block".



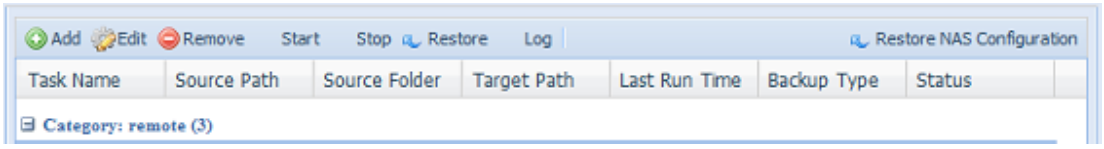
For Thecus product (N8900/N12000/N16000 series) which support JBOD device, the attached JBOD device and his associated disks will also list under the **Disk Information** page. Please see below for a screen shot of a N8900 with a Thecus D16000 attached and installed disks list on.

The JBOD device will have a unique ID that ranges from 1 to 10. The disk no. lead ID will indicate the different JBOD devices. The screen shot below show a JBOD device with ID 4, so J4-6 is indicated under the JBOD device disk list with 6 slots.



Data Guard (Local Backup)

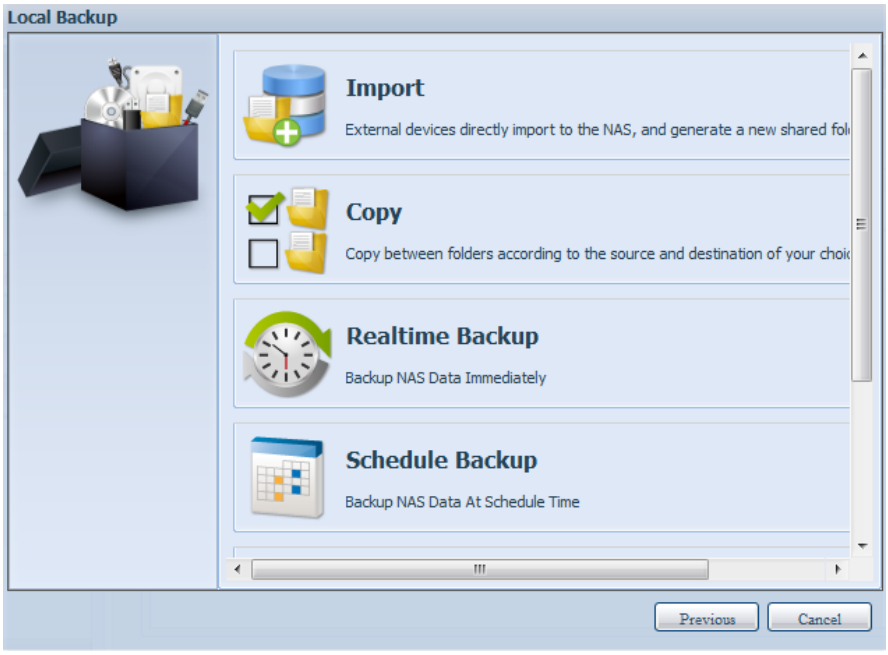
The Thecus product provides complete backup solution between Thecus NAS systems as well as between folders of local systems. For remote data guard backup, please refer to chapter 4, Data Guard (Remote backup).



Remote Data backup	
Item	**Description**
Add	Add a new task.
Edit	Edit selected task.
Remove	Remove selected task.
Start	Click on start to start a scheduled scan task right away.
Stop	Stop the associated running task. Also can be used if a task has been setup as real-time, clicking "Stop" can terminate the running process. Simply click 'Start" to re-start the real-time operation.
Restore	Restore the associated task.
Log	Click to view the associated task process details.
Restore NAS Configuration	Click to restore the system configurations from a selected destination to a source unit.

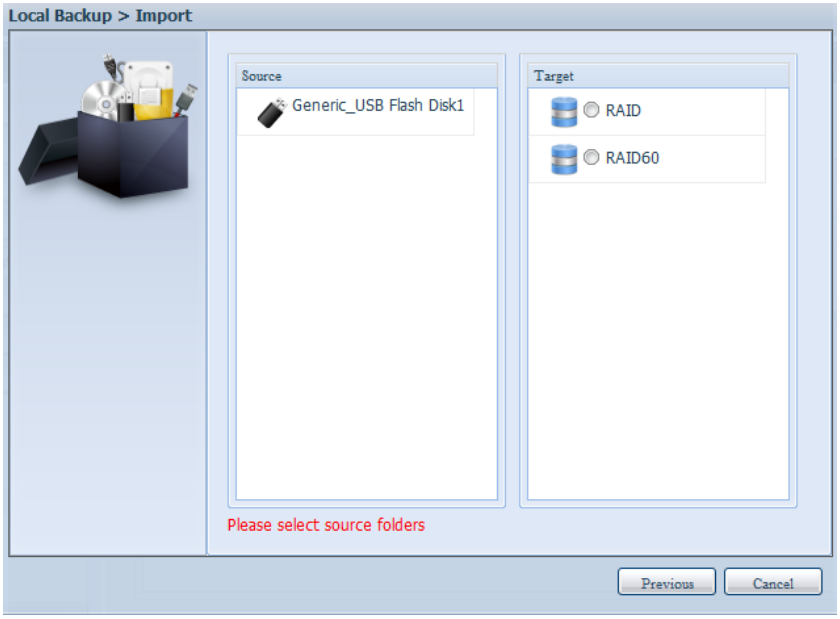
-From the **Data Guard** function list, select **Add.** The data backup setup wizard appears as below, click on "Local Backup":

The local backup has 6 different selection you can choose from.

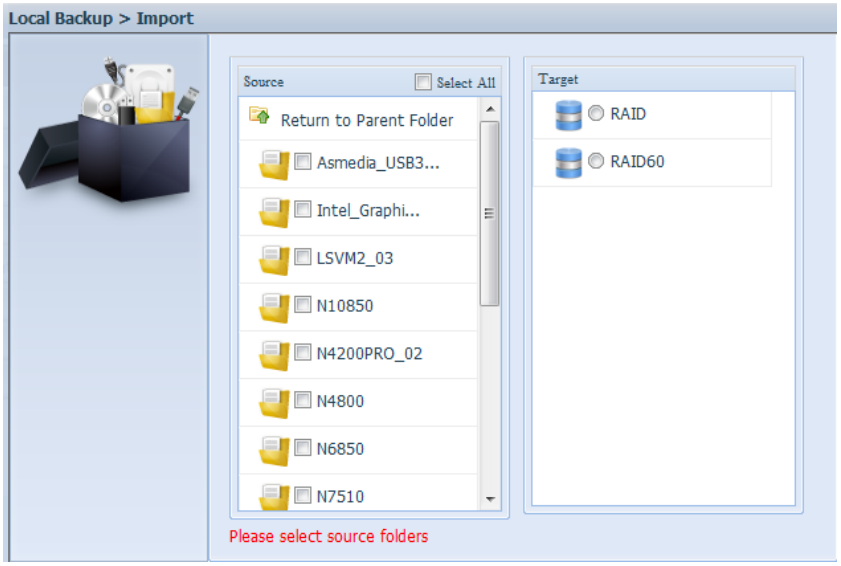

Local Backup
Import
External devices directly import to the NAS, and generate a new shared fol
Copy
Copy between folders according to the source and destination of your choi
Realtime Backup
Backup NAS Data Immediately
Schedule Backup
Backup NAS Data At Schedule Time
Previous
Cancel

Local Data backup	
Item	**Description**
Import	This is associated with external devices which are added to the system such as USB disk. You can select a folder from an external device and import it to the NAS as a share folder.
Copy	Copy folder to folder or NAS folder to external device or external device to NAS folder. This backup is within folder level.
Realtime Backup	The task will be executed on the fly between the source and the target. In other word, any changes made at the source will sync to the destination immediately.
Schedule Backup	The task will be executed on schedule between the source and the target.
iSCSI Backup	The iSCSI volume will be backup to the destination as a single file.
iSCSI Import	The iSCSI file can be imported from the iSCSI backup back to the destination as an iSCSI volume.

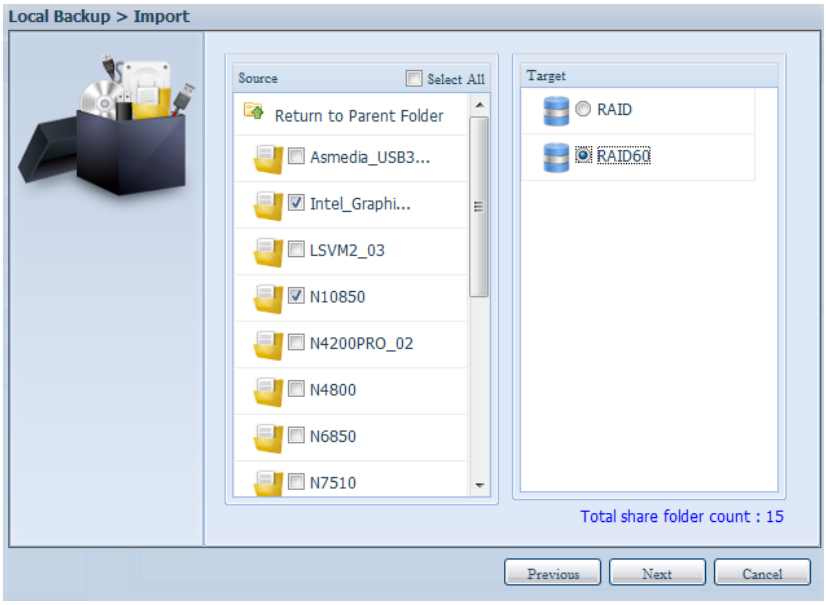
1. **Import:** click on "Import" and a screen will appear as below.
   If there is an external device installed on system such as USB disk, then it will be listed in the Source pane.



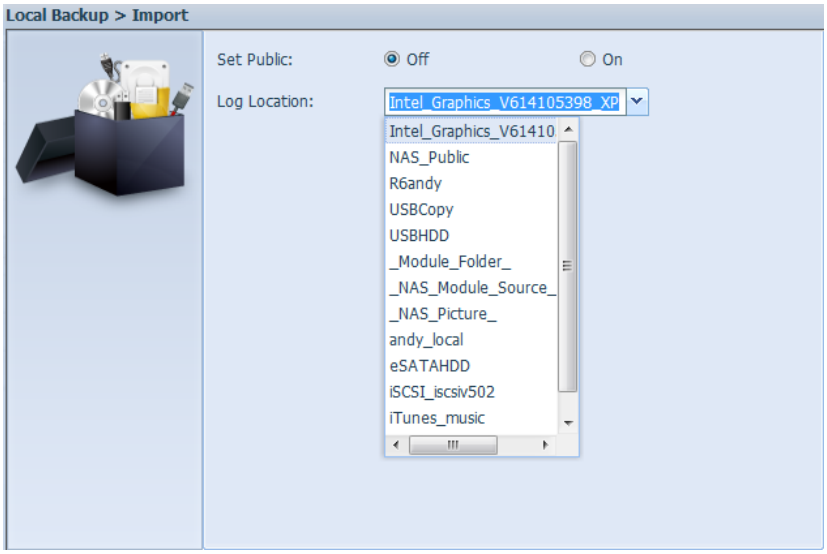
Click on the associated external device and the contain folders will be listed. Select the folders that are going to be imported to the NAS and select the available RAID volume which is listed in Target pane.



In here, we have selected the “Intel Graphi…” and “N10850” folders from the external device and imported them to the NAS under the RAID60volume.

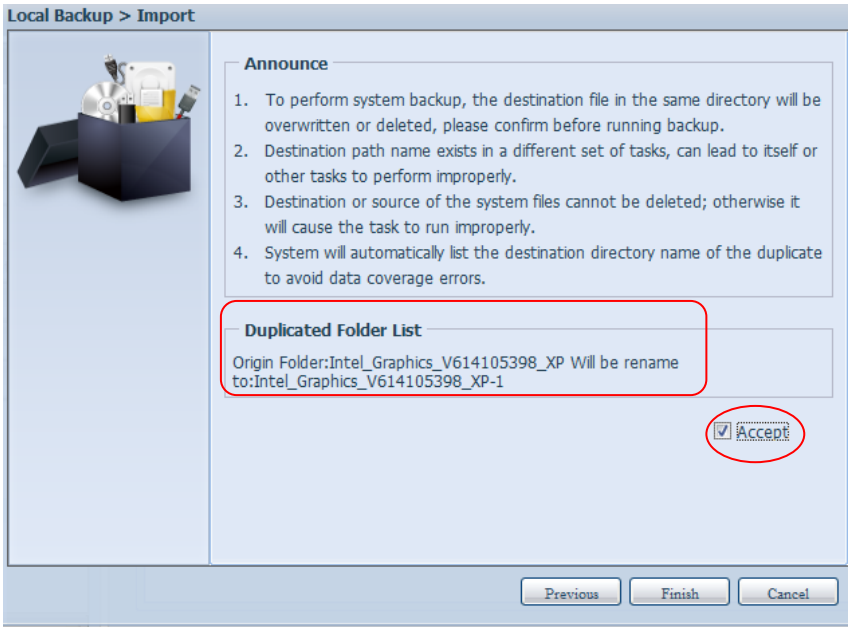


Next, please select the path from the drop down list to save the log. Also, give the access permission whether these selected folders will be “Public” or not after the import.

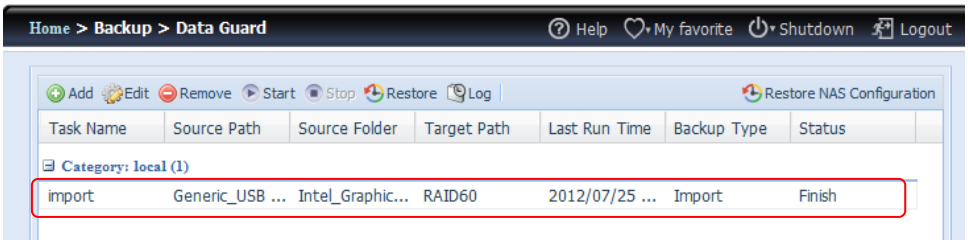


Read the notes and check the "Accept" box for confirmation. If a share name already exists for the import, then the import will be rename automatically to "existing share name -1".

For esample, if the NAS RAID volume "RAID60" already has a folder named "Intel_Graphics_V614105398_XP", the import folder will then be rename to: "Intel_Graphics_V614105398_XP-1".


Local Backup > Import
Announce
1. To perform system backup, the destination file in the same directory will be overwritten or deleted, please confirm before running backup.
2. Destination path name exists in a different set of tasks, can lead to itself or other tasks to perform improperly.
3. Destination or source of the system files cannot be deleted; otherwise it will cause the task to run improperly.
4. System will automatically list the destination directory name of the duplicate to avoid data coverage errors.
Duplicated Folder List
Origin Folder:Intel_Graphics_V614105398_XP Will be rename to:Intel_Graphics_V614105398_XP-1
Accept
Previous
Finish
Cancel

Now, you will see in the data guard task list that you have created a task .

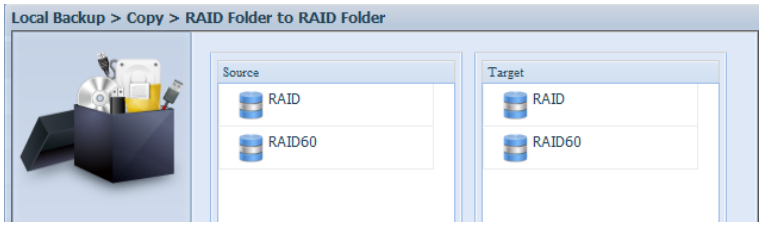


And that the system has created 2 new share folders from the task just created.

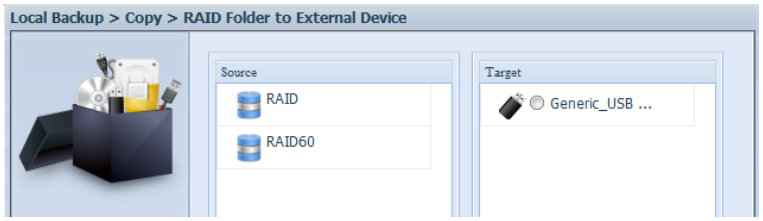
2. **Copy:** click on "Copy" and this screen appears.
   3 different options can be selected, folder to folder, folder to external device or external device to folder.

Local Backup > Copy
RAID Folder -> RAID Folder
To select more than one folder to copy to a single destination fold
RAID Folder -> External Device
To select more than one folder to copy to a single external device
External Device -> RAID Folder
Choose external device to copy to a single folder
Previous
Cancel

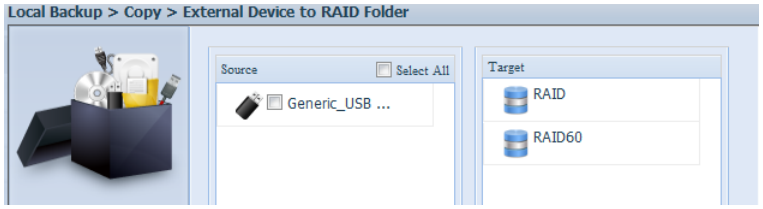
Folder to Folder



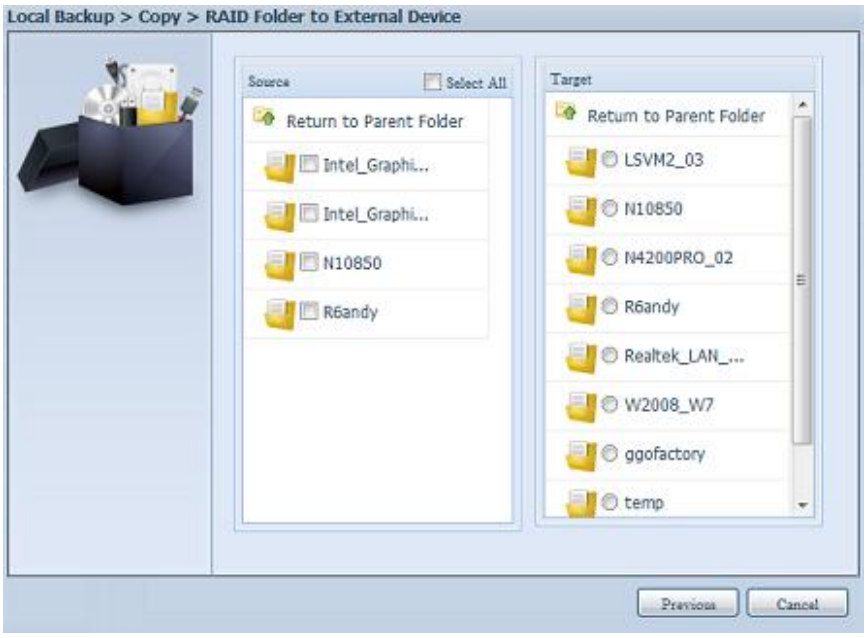
Folder to external device



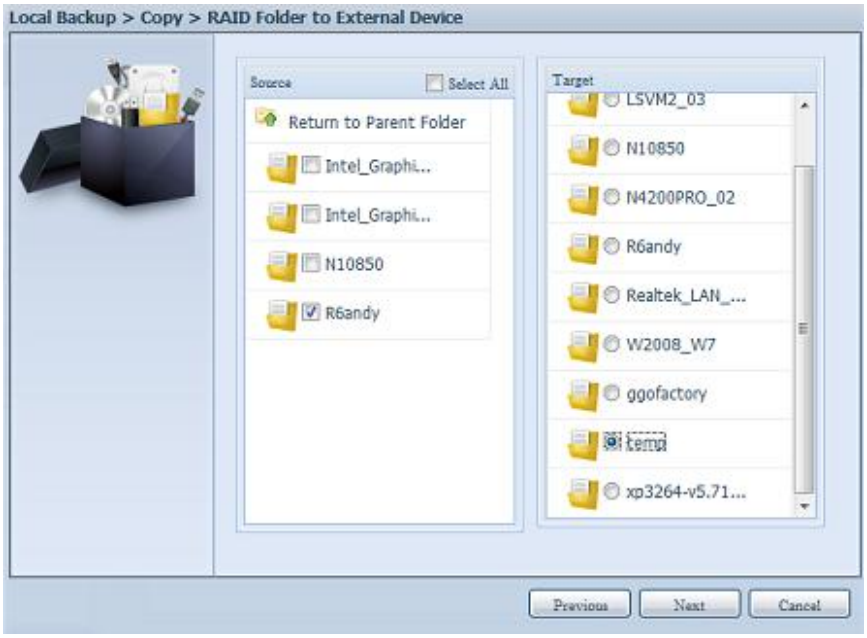
External device to Folder



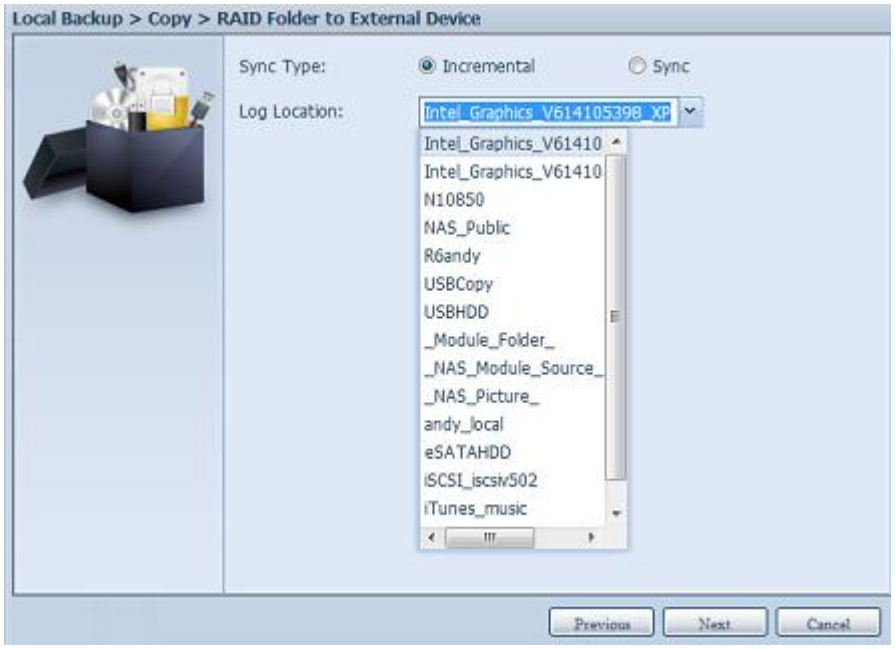
Let’s take “Folder to External device” as an example. In the source pane, select the desired RAID volume and its associated folder list will appear; same method in the target pane for the associated external device.



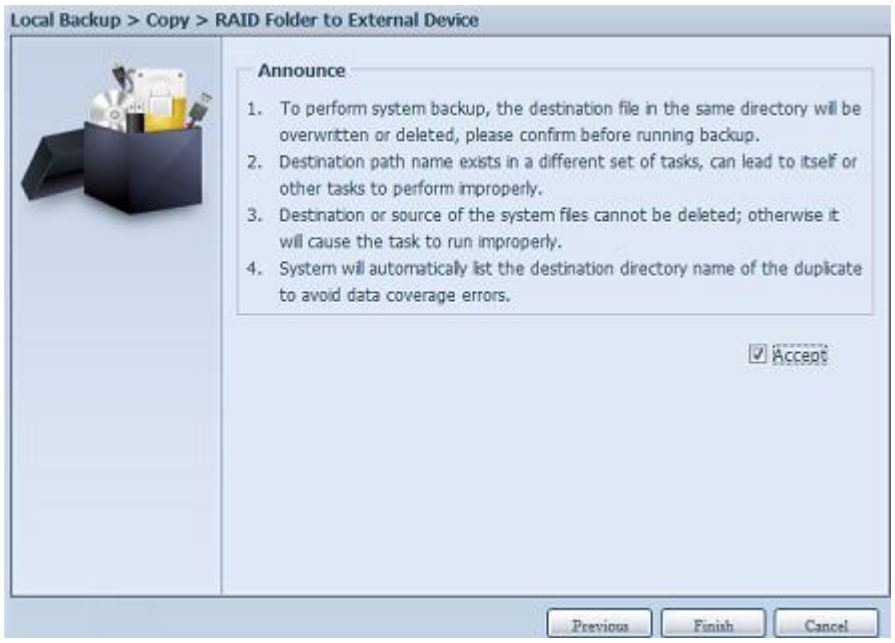
Select a folder from the source pane which is going to be copy over, then select in target pane it’s destination.



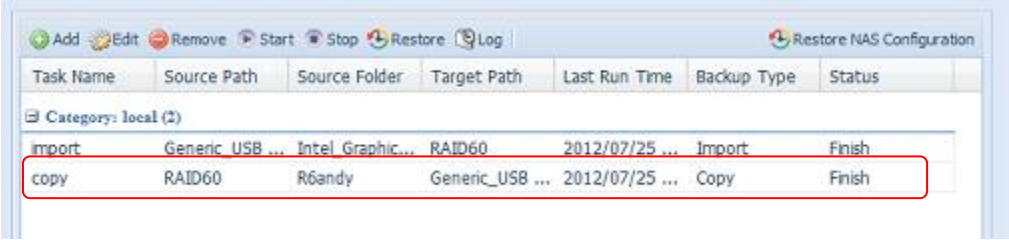
Choosing the sync type, “Incremental” or ‘Sync”, and select the log path from the drop menu list.



Read the notes and check the “Accept” box for confirmation.

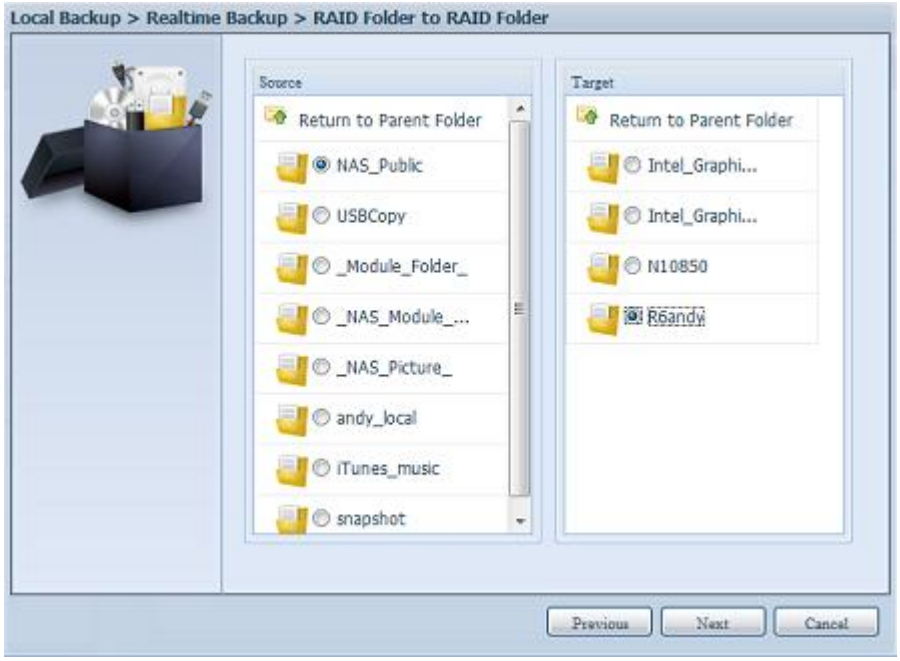

Local Backup > Copy > RAID Folder to External Device
Announce
1. To perform system backup, the destination file in the same directory will be overwritten or deleted, please confirm before running backup.
2. Destination path name exists in a different set of tasks, can lead to itself or other tasks to perform improperly.
3. Destination or source of the system files cannot be deleted; otherwise it will cause the task to run improperly.
4. System will automatically list the destination directory name of the duplicate to avoid data coverage errors.
Accept
Previous
Finish
Cancel

Now, you will see in the data guard task list that you have created a task.

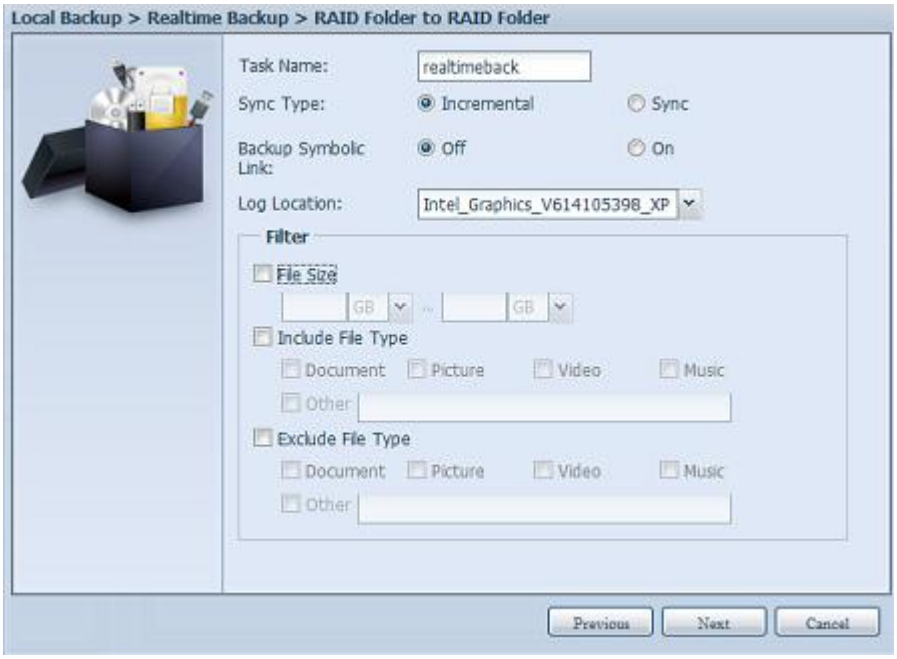


3. **Realtime Backup:** click on "Realtime Backup" and this screen will appear. 2 different options can be selected from, folder to folder, folder to external device.

   Let's take "Folder to Folder" backup for example. Select from the source pane the folder "NAS_Public", then select its destination in the target panefolder "R6andy".

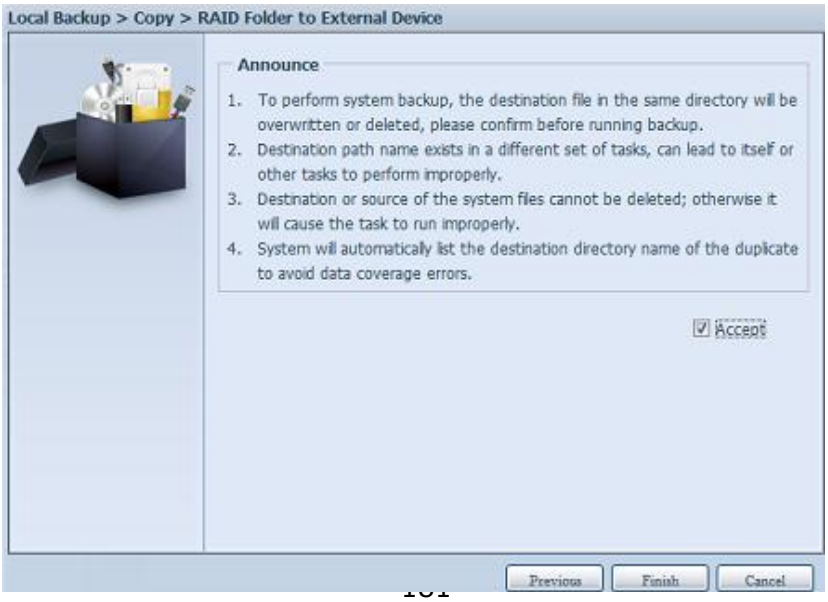


Next, fill in the task name and related settings.

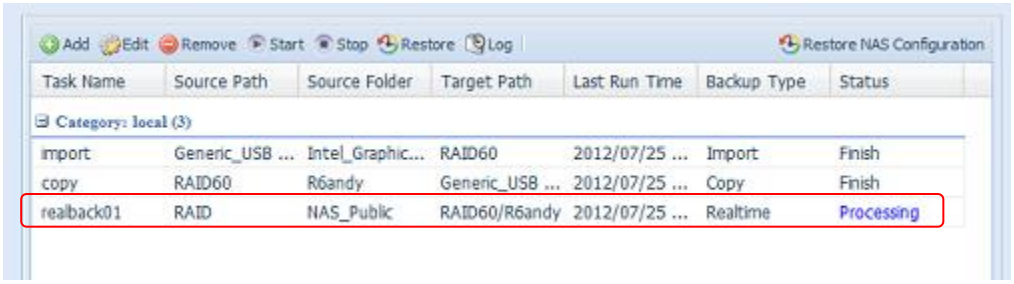


Realtime Backup	
Item	**Description**
Task Name	Input the task name, length limited to 4~12 characters.
Sync Type	Select "Incremental" or "Synchronize".
Backup Symbolic Link	Choose to backup symbolic link which is included in the source.
Filter	The filter can be set to be executed only in certain circumstances. If none of them has been selected, it will do the real time backup from the source to the destination in full. File size: From xx ~ xxx If xx=1 and xxx blank then only file size > xx will execute real time backup. If xx=1 and xxx=2 then only size in between xx and xxx will execute real time backup. If xx blank and xxx=2 then only file size < xxx will execute real time backup. Include File Type: Only the associated file format will do the real time backup. Exclude File Type: The excluded file format won't be included in the real time backup. **For document file format:** doc, xls, pdf, docx, xlsx, txt, ppt, pptx, html, htm **For picture file format:** jpg, bmp, tif, png, pbm, tga, xar, xbm **For video file format:** avi, mpg, mp4, mkv, fli, flv, rm, ram **For music file format**: mp3, wav, wma, acc, dss, msv, dvf, m4p, 3gp, amr, awb User defined can be input in other box.

Read the notes and check the "Accept" box for confirmation.

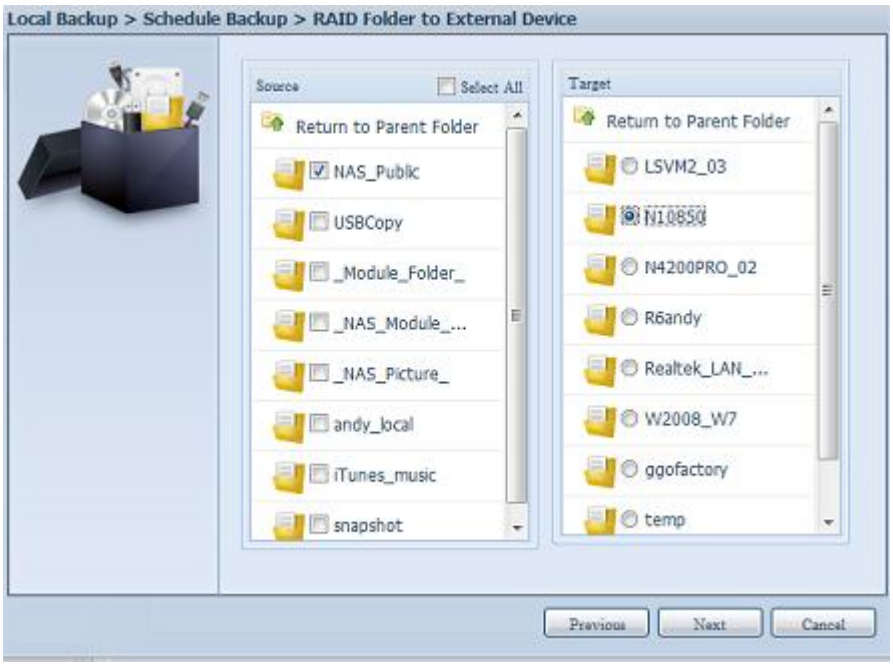

Local Backup > Copy > RAID Folder to External Device
Announce
1. To perform system backup, the destination file in the same directory will be overwritten or deleted, please confirm before running backup.
2. Destination path name exists in a different set of tasks, can lead to itself or other tasks to perform improperly.
3. Destination or source of the system files cannot be deleted; otherwise it will cause the task to run improperly.
4. System will automatically list the destination directory name of the duplicate to avoid data coverage errors.
Accept
Previous
Finish
Cancel

Now, you can see in the data guard task list that your created task is listed. The task status will say "Processing" untill the "Stop" button is pressed.



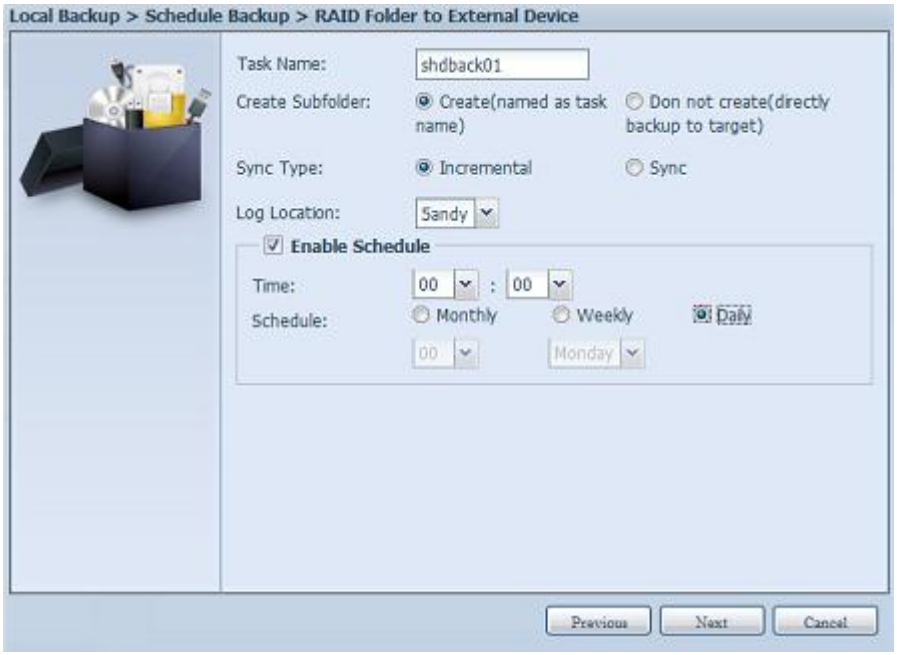
4. **Schedule Backup:** click on "Schedule Backup" and this screen will. 2 different choices can be selected from, folder to folder, folder to external device.

   Let's use "Folder to External device" backup for our example. From the NAS volume RAID in the Source pane select the folder "NAS_Public", then in the target pane select the external USB disk folder "N10850".

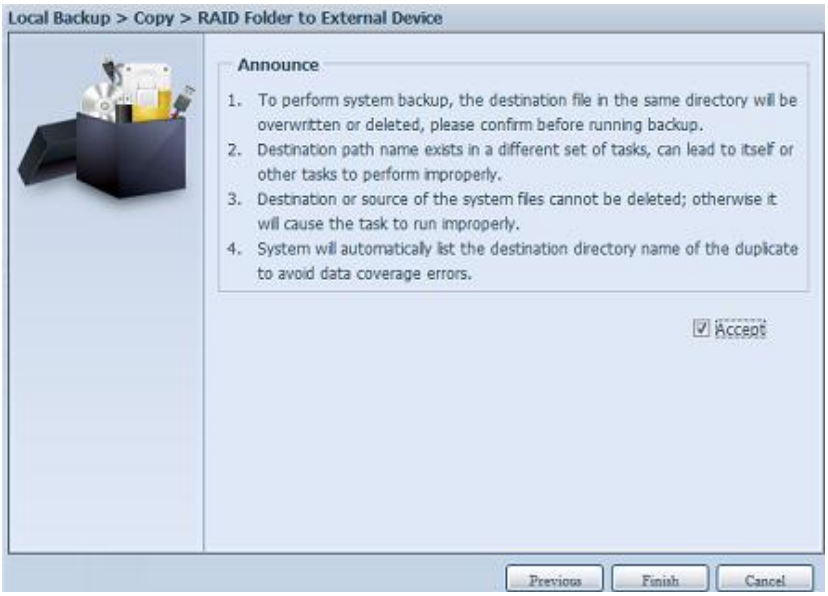


   Next, fill in the task name and related settings.

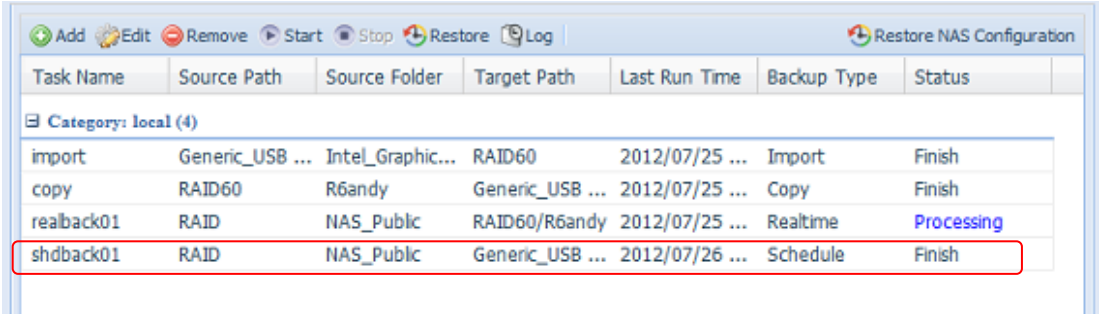
Schedule Backup	
Item	**Description**
Task Name	Input the task name, length limited to 4~12 characters.
Create Sub-folder	If you choose to create a sub-folder, then it will use the task name as folder name then copy the source under it. Or it will copy the source to the same level as the destination.
Sync Type	Select "Incremental" or "Synchronize".
Log Location	Select from the drop down list where the task log will be stored.
Enable Schedule	Click to enable. If it is not checked, the task won't start unless you select the associate task and click "Start" from the task list page.
Time	Specify the time for the backup to start.
Schedule	Can choose daily, weekly or monthly.



Read the notes and check the "Accept" box for confirmation.


Local Backup > Copy > RAID Folder to External Device
Announce
1. To perform system backup, the destination file in the same directory will be overwritten or deleted, please confirm before running backup.
2. Destination path name exists in a different set of tasks, can lead to itself or other tasks to perform improperly.
3. Destination or source of the system files cannot be deleted; otherwise it will cause the task to run improperly.
4. System will automatically list the destination directory name of the duplicate to avoid data coverage errors.
Accept
Previous
Finish
Cancel

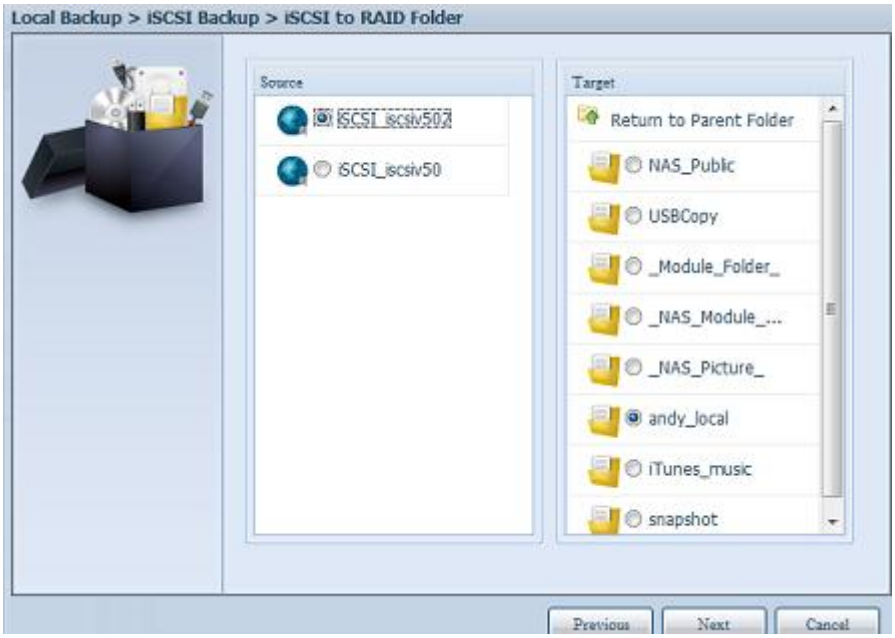
Now, you will see in the data guard task list that you have created a task.



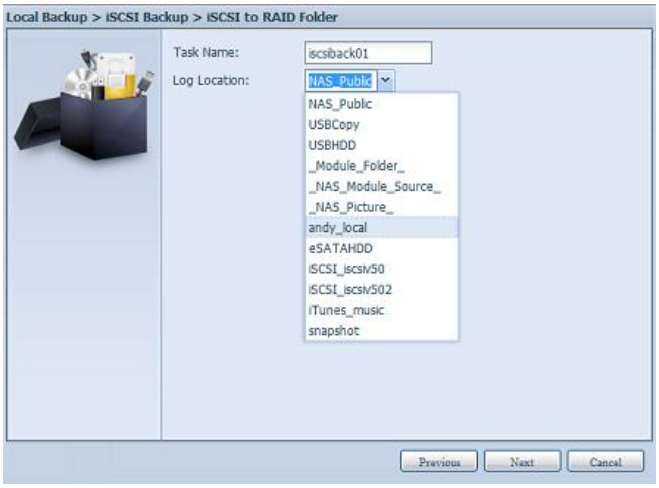
5. **iSCSI Backup:** click on "iSCSI Backup" and screen appear as below.
   It can be backup to two different storage pool, iSCSI to folder, iSCSI to external device.

   Let's take example to have "iSCSI to Folder" backup, from existed iSCSI volume "iSCSI_iscsiv502" to volume RAID folder "andy_local".

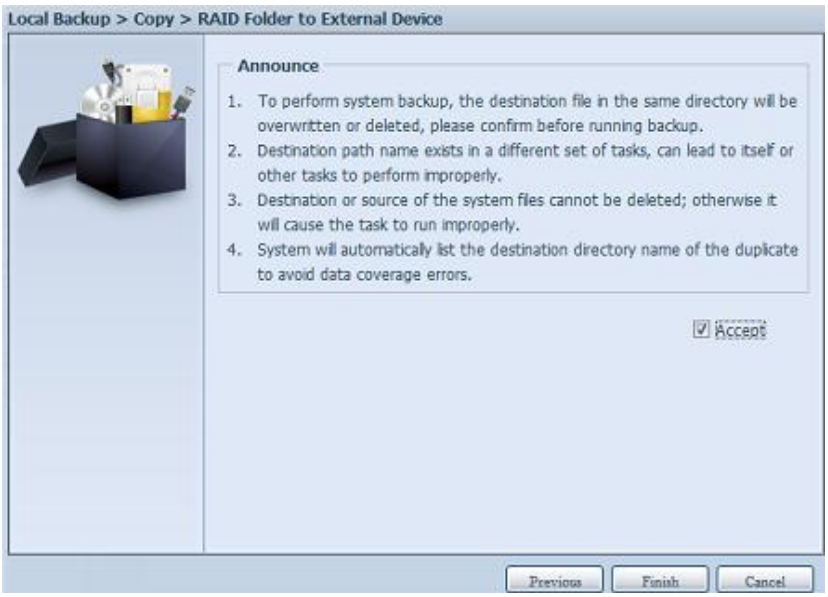
   The source pane listed "iSCSI_iscsiv502" and "iSCSI_iscsiv50" where are iscsi volume has existed in this system with name "iSCSI_+iscsi target volume name".



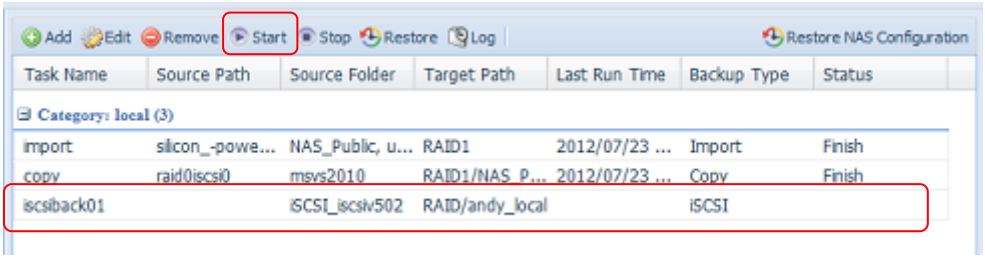
Next, provide the task name and where the task log will store.



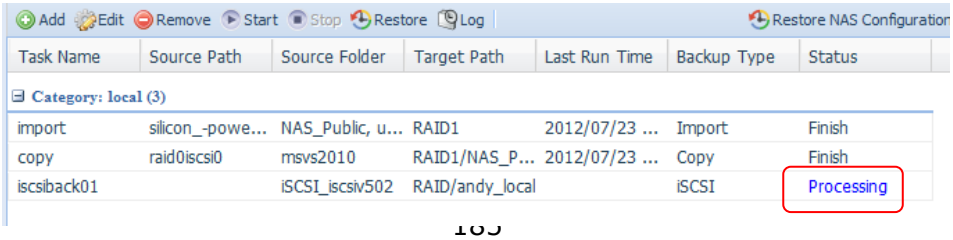
Reading the note and check on "Accept" for confirmation.


Local Backup > Copy > RAID Folder to External Device
Announce
1. To perform system backup, the destination file in the same directory will be overwritten or deleted, please confirm before running backup.
2. Destination path name exists in a different set of tasks, can lead to itself or other tasks to perform improperly.
3. Destination or source of the system files cannot be deleted; otherwise it will cause the task to run improperly.
4. System will automatically list the destination directory name of the duplicate to avoid data coverage errors.
Accept
Previous
Finish
Cancel

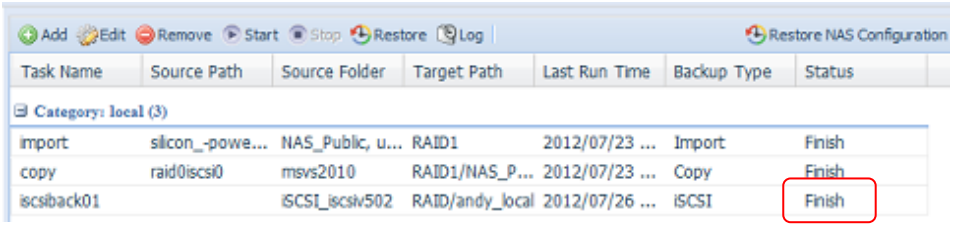
Now, from the data guard task list will have created task listed. To start the iSCSI volume backup, select the task and click "Start" from task bar.



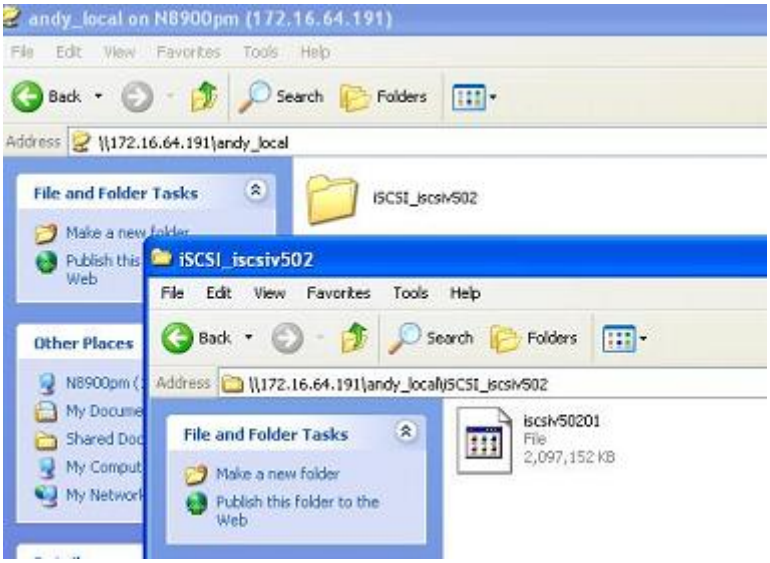
Once "Start" click, the associated iSCSI volume will not allow to I/O during backup processing. And the task status will change to 'Processing".



States change to “Finish” after task complete.

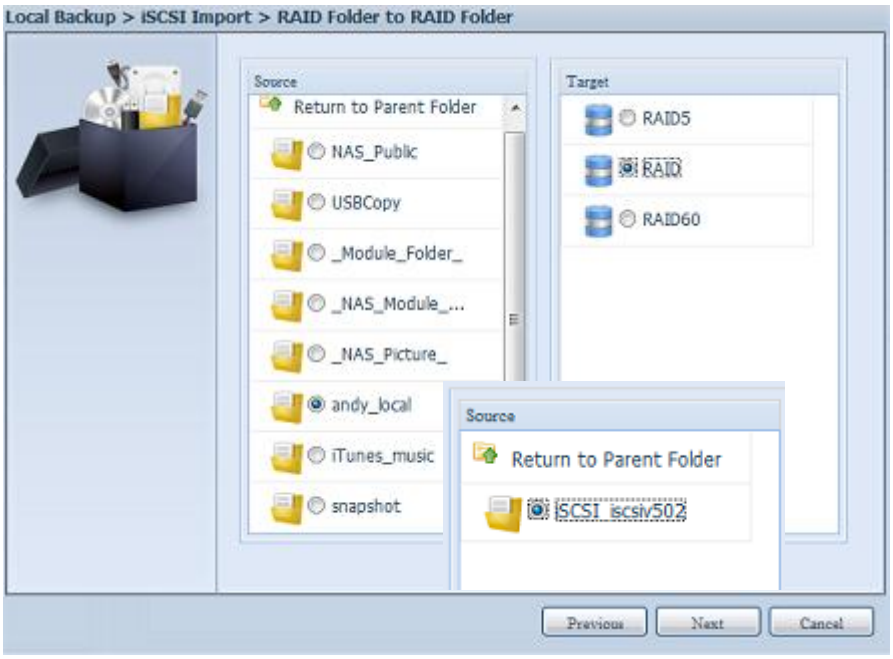


From the RAID volume folder ‘andy_local’, it has backup iSCSI volume file stored. This backup iSCSI volume file is needed while it required import to storage. Next topic will describe about this.

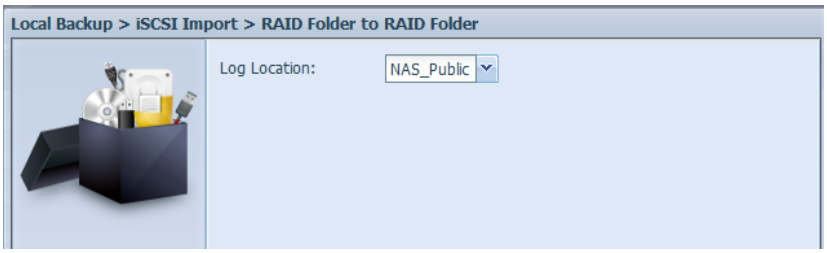


6. **iSCSI Import:** click on “iSCSI Import” and screen appear as below.
   It can be imported from two different storage pools, folder to iSCSI or external device to iSCSI. It is depend on where iSCSI volume has backup to.

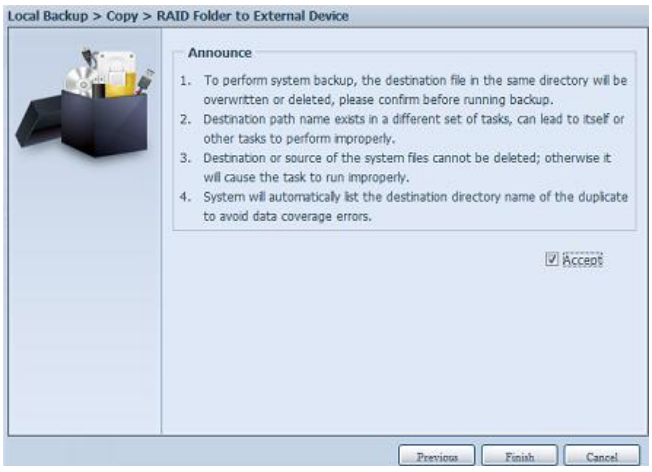
   Let’s take example to import “RAID folder to iSCSI” which is the iSCSI volume we have backup earlier to RAID volume folder andy_local than import to volume RAID.



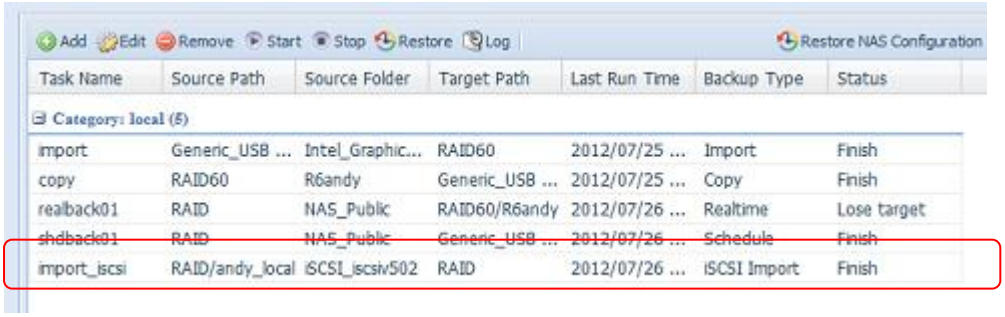
Next, provide where the task log will store.



Reading the note and check on "Accept" for confirmation.


Local Backup > Copy > RAID Folder to External Device
Announce
1. To perform system backup, the destination file in the same directory will be overwritten or deleted, please confirm before running backup.
2. Destination path name exists in a different set of tasks, can lead to itself or other tasks to perform improperly.
3. Destination or source of the system files cannot be deleted; otherwise it will cause the task to run improperly.
4. System will automatically list the destination directory name of the duplicate to avoid data coverage errors.
Accept
Previous
Finish
Cancel

Now, from the data guard task list will have created task listed.



Volume Expansion Management

The user guide please refers to URL below.
http://www.thecus.com/download/manual/AllinOne_64bit/Volume_Expansion_v1.0.pdf

Appendix A: Customer Support

If your Thecus IP storage is not working properly, we encourage you to check out **Chapter 6: Troubleshooting**, located in this manual. You can also try to ensure that you are using the latest firmware version for your Thecus IP storage. Thecus is committed to providing free firmware upgrades to our customers. Our newest firmware is available on our Download Center:

http://www.thecus.com/download.php

If you are still experiencing problems with your Thecus IP storage, or require a Return Merchandise Authorization (RMA), feel free to contact technical support via our Technical Support Website:

http://www.thecus.com/support_tech.php

Customers in the US should send all technical support enquiries to the US contact window included in the following web page:

http://www.thecus.com/support_tech.php

For Sales Information you can e-mail us at:

sales@thecus.com

Thank you for choosing Thecus!

Appendix B: RAID Basics

Overview

A Redundant Array of Independent Disks (RAID) is an array of several hard disks that provide data security and high performance. A RAID system accesses several hard disks simultaneously, which improves I/O performance over a single hard disk. Data security is enhanced by a RAID, since data loss due to a hard disk failure is minimized by regenerating redundant data from the other RAID hard disks.

Benefits

RAID improves I/O performance, and increases data security through fault tolerance and redundant data storage.

Improved Performance

RAID provides access to several hard disk drives simultaneously, which greatly increases I/O performance.

Data Security

Hard disk drive failure unfortunately is a common occurrence. A RAID helps prevent against the loss of data due to hard disk failure. A RAID offers additional hard disk drives that can avert data loss from a hard disk drive failure. If a hard drive fails, the RAID volume can regenerate data from the data and parity stored on its other hard disk drives.

RAID Levels

The Thecus IP storage supports standard RAID levels 0, 1, 5, 6, 10, 50, 60 and JBOD. You choose a RAID level when you create a system volume. The factors for selecting a RAID level are:

- Your requirements for performance
- Your need for data security
- Number of hard disk drives in the system, capacity of hard disk drives in the system

The following is a description of each RAID level:

RAID 0

RAID 0 is best suited for applications that need high bandwidth but do not require a high level of data security. The RAID 0 level provides the best performance of all the RAID levels, but it does not provide data redundancy.

RAID 0 uses disk striping and breaking up data into blocks to write across all hard drives in the volume. The system can then use multiple hard drives for faster read and write. The stripe size parameter that was set when the RAID was created determines the size of each block. No parity calculations complicate the write operation.

RAID 1

RAID 1 mirrors all data from one hard disk drive to a second one hard disk drive, thus providing complete data redundancy. However, the cost of data storage capacity is doubled.

This is excellent for complete data security.

RAID 5

RAID 5 offers data security and it is best suited for networks that perform many small I/O transactions at the same time, as well as applications that require data security such as office automation and online customer service. Use it also for applications with high read requests but low write requests.

RAID 5 includes disk striping at the byte level and parity information is written to several hard disk drives. If a hard disk fails the system uses parity stored on each of the other hard disks to recreate all missing information.

RAID 6

RAID 6 is essentially an extension of RAID level 5 which allows for additional fault tolerance by using a second independent distributed parity scheme (dual parity) Data is striped on a block level across a set of drives, just like in RAID 5, and a second set of parity is calculated and written across all the drives; RAID 6 provides for an extremely high data fault tolerance and can sustain two simultaneous drive failures.

This is a perfect solution for mission critical applications.

RAID 10

RAID 10 is implemented as a striped array whose segments are RAID 1 arrays.
RAID 10 has the same fault tolerance as RAID level 1.
RAID 10 has the same overhead for fault-tolerance as mirroring alone. High I/O rates are achieved by striping RAID 1 segments.
Under certain circumstances, RAID 10 array can sustain up to 2 simultaneous drive failures

Excellent solution for applications that would have otherwise gone with RAID 1 but need an additional performance boost.

RAID 50

A RAID 50 combines the straight block-level striping of RAID 0 with the distributed parity of RAID 5. This is a RAID 0 array striped across RAID 5 elements. It requires at least 6 drives.

RAID 60

A RAID 60 combines the straight block-level striping of RAID 0 with the distributed double parity of RAID 6. That is, a RAID 0 array striped across RAID 6 elements. It requires at least 8 disks.

JBOD

Although a concatenation of disks (also called JBOD, or "Just a Bunch of Disks") is not one of the numbered RAID levels, it is a popular method for combining multiple physical disk drives into a single virtual one. As the name implies, disks are merely concatenated together, end to beginning, so they appear to be a single large disk.

As the data on JBOD is not protected, one drive failure could result total data loss.

Stripe Size

The length of the data segments being written across multiple hard disks. Data is written in stripes across the multiple hard disks of a RAID. Since multiple disks are accessed at the same time, disk striping enhances performance. The stripes can vary in size.

Disk Usage

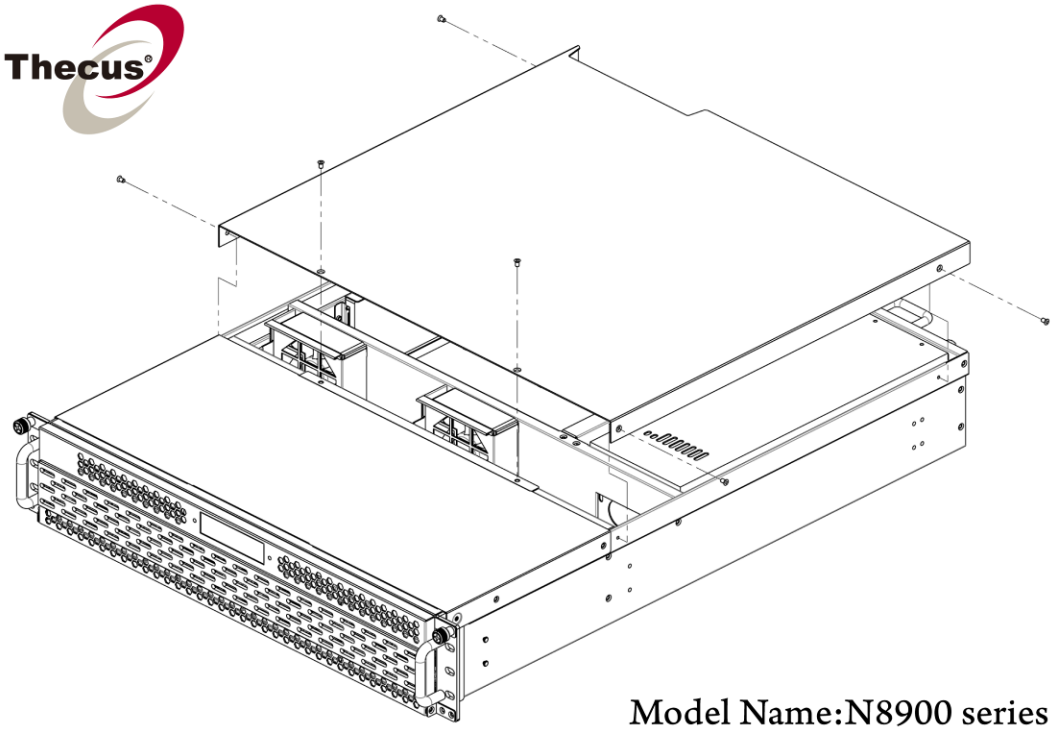
When all disks are of the same size, and used in RAID, Thecus IP storage disk usage percentage is listed below:

RAID Level	Percentage Used
RAID 0	100%
RAID 1	1/n x 100%
RAID 5	(n-1)/n x 100%
RAID 6	(n-2)/n x 100%
RAID 10	50%
RAID 50	(n-1)/n x 100%
RAID 60	(n-2)/n x 100%
JBOD	100%

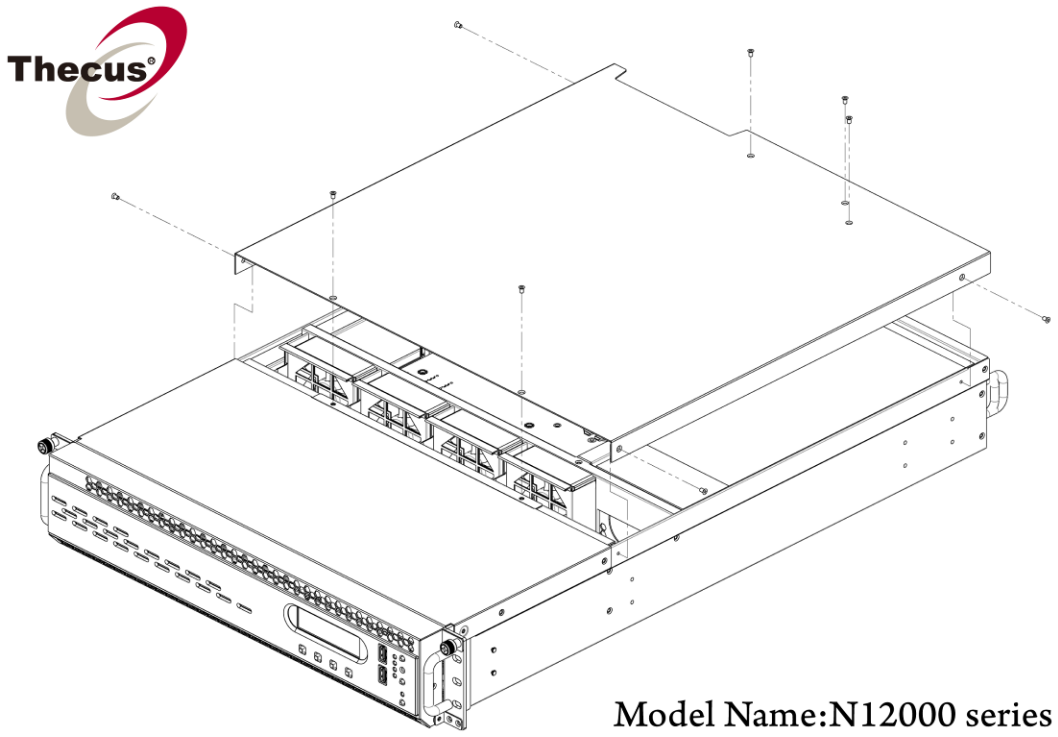
n：HDD number

Appendix C: How to open the top cover

N8900 series:

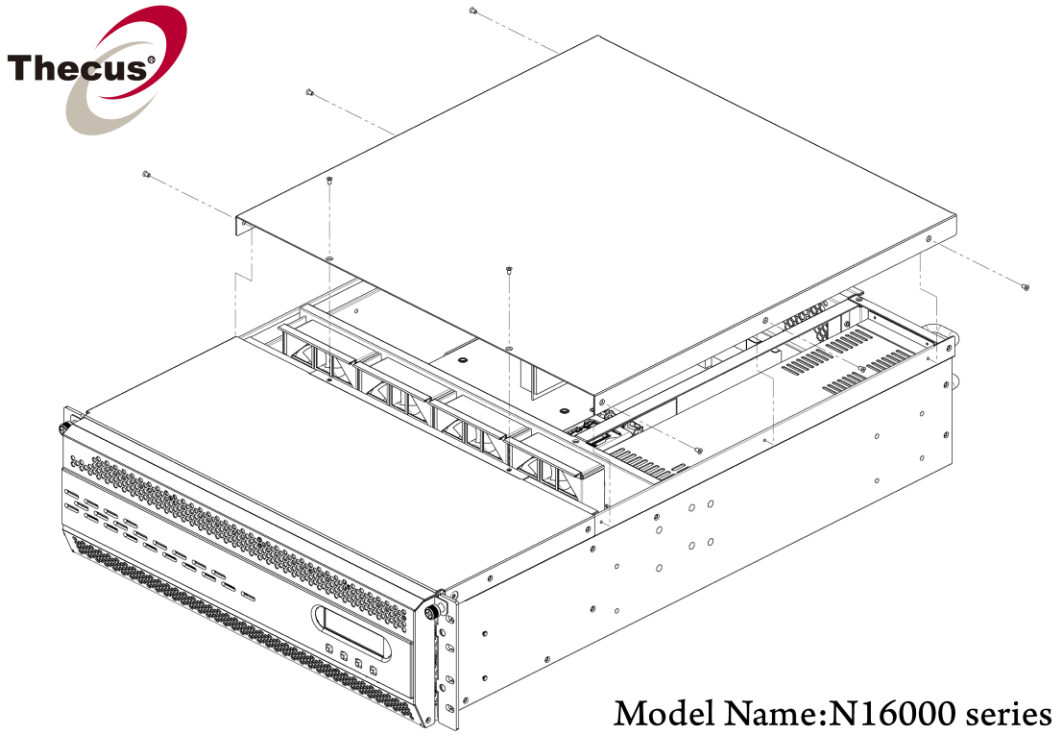


N12000 series:



Model Name:N12000 series

N16000 series:



Model Name:N16000 series

Appendix D: Active Directory Basics

Overview

With Windows 2000, Microsoft introduced Active Directory (ADS), which is a large database/information store. Prior to Active Directory the Windows OS could not store additional information in its domain database. Active Directory also solved the problem of locating resources; which previously relied on Network Neighborhood, and was slow. Managing users and groups were among other issues Active Directory solved.

What is Active Directory?

Active Directory was built as a scalable, extensible directory service that was designed to meet corporate needs. A repository for storing user information, accounts, passwords, printers, computers, network information and other data, Microsoft calls Active Directory a "namespace" where names can be resolved.

ADS Benefits

ADS lets Thecus IP storage integrate itself with the existing ADS in an office environment. This means the Thecus IP storage is able to recognize your office users and passwords on the ADS server. Other major benefits ADS support provides include:

1. Easy integration of Thecus IP storage into the existing office IT infrastructure

   The Thecus IP storage acts as a member of the ADS. This feature significantly lowers the overhead of the system administrator. For example, corporate security policies and user privileges on an ADS server can be enforced automatically on Thecus IP storage.

2. Centralized user/password database

   The Thecus IP storage does not maintain its own copy of the user/password database. This avoids data inconsistency between Thecus IP storage and other servers. For example, without ADS support, an administrator might need to remove a specific user privilege on Thecus IP storage and each individual server. With ADS support, the change on an ADS server is known to all of its ADS members.

Appendix E: Licensing Information

Overview

This product included copyrighted third-party software licensed under the terms of GNU General Public License. Please see THE GNU General Public License for extra terms and conditions of this license.

Source Code Availability

Thecus Technology Corp. has exposed the full source code of the GPL licensed software. For more information on how you can obtain our source code, please visit our web site, http://www.thecus.com.

Copyrights

- This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).
- This product includes software developed by Mark Murray.
- This product includes software developed by Eric Young (eay@cryptsoft.com).
- This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).
- This product includes PHP, freely available from (http://www.php.net/).
- This product includes software developed by the University of California, Berkeley and its contributors.
- This product includes software developed by Winning Strategies, Inc.
- This product includes software developed by the Apache Group for use in the Apache HTTP server project (http://www.apache.org/).
- This product includes software developed by Softweyr LLC, the University of California, Berkeley, and its contributors.
- This product includes software developed by Bodo Moeller.
- This product includes software developed by Greg Roelofs and contributors for the book, "PNG: The Definitive Guide," published by O'Reilly and Associates.
- This product includes software developed by the NetBSD Foundation, Inc. and its contributors.
- This product includes software developed by Yen Yen Lim and North Dakota State University.
- This product includes software developed by the Computer Systems Engineering Group at Lawrence Berkeley Laboratory.
- This product includes software developed by the Kungliga Tekniska Högskolan and its contributors.
- This product includes software developed by the Nick Simicich.
- This product includes software written by Tim Hudson (tjh@cryptsoft.com).
- This product includes software developed by Christopher G. Demetriou for the NetBSD Project.

CGIC License Terms

Basic License

CGIC, copyright 1996, 1997, 1998, 1999, 2000, 2001, 2002, 2003, 2004 by Thomas Boutell and Boutell.Com, Inc.

Permission is granted to use CGIC in any application, commercial or noncommercial, at no cost. HOWEVER, this copyright paragraph must appear on a "credits" page accessible in the public online and offline documentation of the program. Modified versions of the CGIC library should not be distributed without the attachment of a clear statement regarding the author of the modifications, and this notice may in no case be removed. Modifications may also be submitted to the author for inclusion in the main CGIC distribution.

GNU General Public License

Version 2, June 1991

Copyright © 1989, 1991 Free Software Foundation, Inc.
51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

PREAMBLE

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software
Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is

modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another Language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

   Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program).

   Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

   You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

   a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

   b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

   c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate

copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

   a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

   b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

   c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

   The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

   If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even

though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

   If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

   It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

   This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is

permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

   Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS